HACKING SECRETS REVEALED

Information and Instructional Guide

HACKING SECRETS REVEALED

Table of Contents

DISCLAIMER

The authors of this manual will like to express our concerns about the misuse of the information contained in this manual. By purchasing this manual you agree to the following stipulations. Any actions and or activities related to the material contained within this manual is solely your responsibility.

The misuse of the information in this manual can result in criminal charges brought against the persons in question. The authors will not be held responsible in the event any criminal charges be brought against any individuals misusing the information in this manual to break the law.

(Note This manual was created for Information purposes only.)

Introduction

THE internet is ever growing and you and I are truly pebbles in a vast ocean of information. They say what you don't know can't hurt you. When it comes to the Internet believe quite the opposite. On the Internet there a millions and millions of computer users logging on and off on a daily basis. Information is transferred from one point to another in a heartbeat. Amongst those millions upon millions of users, there's you.

As humble a user you may be of the Internet, you are pitted against the sharks of the information super highway daily. Problem with that is the stealth by which it happens. Currently about 30-40% of all users are aware of the happenings on their computer. The others simply either don't care or don't have the proper "know how" to recognize if their system is under attack and or being used.

You bought this manual because you are concerned about your privacy on the Internet. As well you should be. On the Internet nothing is quite what it appears to be. The uninformed will get hurt in many ways.

By taking interest in your privacy and safety, you have proven yourself to be above the rest. You can never have enough information. Information is power and the more informed you as a user become the less likely you are to fall prey to the sharks of the Internet.

In this manual, I will cover with you things that may scare you. Some things may even make you paranoid about having a computer. Don't be discouraged though, as I will also tell you how to protect yourself. The reasons for telling you the "dirt" if you will is that I feel it important for you to know what is at risk.

I wrote this manual as a guide. To show you how hackers gain access to your system using security flaws and programs. The theory goes that if you are aware of what they are doing and how they are doing it you'll be in a much better position to protect yourself from these attacks.

(Through out this manual you will see reference to the term "Hacker." This is a term I use very loosely for these individuals.)

These are just a few of the topics that will be covered:

- How "hackers" get into your system
- What tools they use
- How a hacker can effectively "Bug" your house via your computer. (Don't believe me, read on you'll be very surprised)
- What information they have access to. And why you should try to protect yourself. (You might be surprised to find out what they know.)
- Tips and tricks that hackers use
- How your Antivirus software alone is not enough
- What to look for if you suspect you're being hacked
- What the greatest flaw to all computers are
- And more…

By no means am I going to make a ludicrous claim that this manual will protect you from everything. What I will say is that by reading this manual hopefully you will be in a better situation to protect yourself from having your information compromised.

Did you know it doesn't matter if you're connected to the net 24hrs a day or 15 min's a day your system is vulnerable. Not only is it vulnerable in that 15 min's you can possibly loose all your data get locked out of your own system and have all your confidential information like your "Bank Account Numbers", "Your Budget", "Your personal home address" compromised.

Don't give me wrong, I'm not trying to throw you into a state of paranoia either. What I am saying is that if you're not careful you leave yourself open to a wide range of attacks.

Perhaps you're skeptical and saying to yourself "Oh I don't do anything on the net except check my E-mail etc that sort of thing can't happen to me."

Okay I like a challenge let's do a test!

Chapter

1

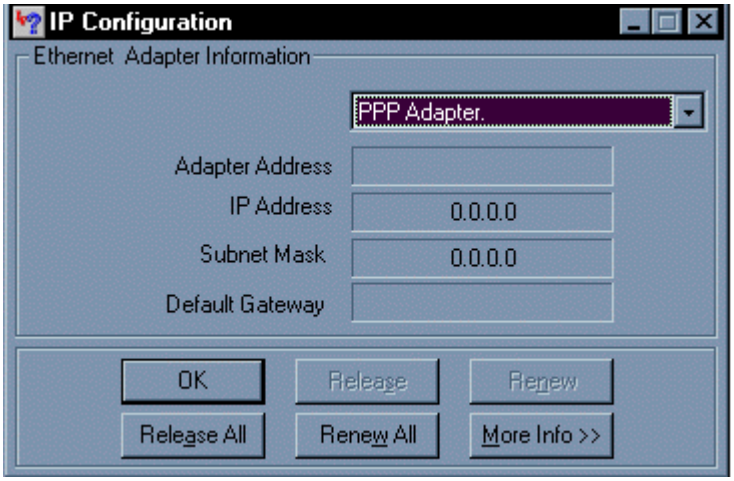
SYSTEM INTRUSION IN 15 SECONDS

System intrusion in 15 seconds, that's right it can be done. If you possess certain security flaws your system can be broken into in less that 15 seconds.

To begin this chapter I'd like you to do the following. Connect to the Internet using your dial up account if you are on dial up. If you are on dedicated service like High Speed connections (ie, Cable and DSL) then just proceed with the steps below.

- Click **Start**
- Go to **Run**
- Click **Run** (It's a step by step manual) :-)
- Type **Winipcfg**
- Hit the **Enter** Key

This should bring up a window that looks like the following

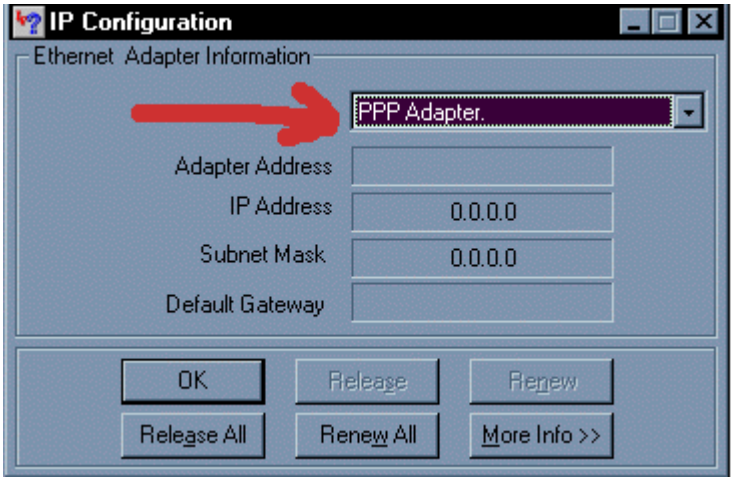


* For editorial reason the above info has been omitted *

What you should see under IP address is a number that looks something like this.

207.175.1.1 (The number will be different.)

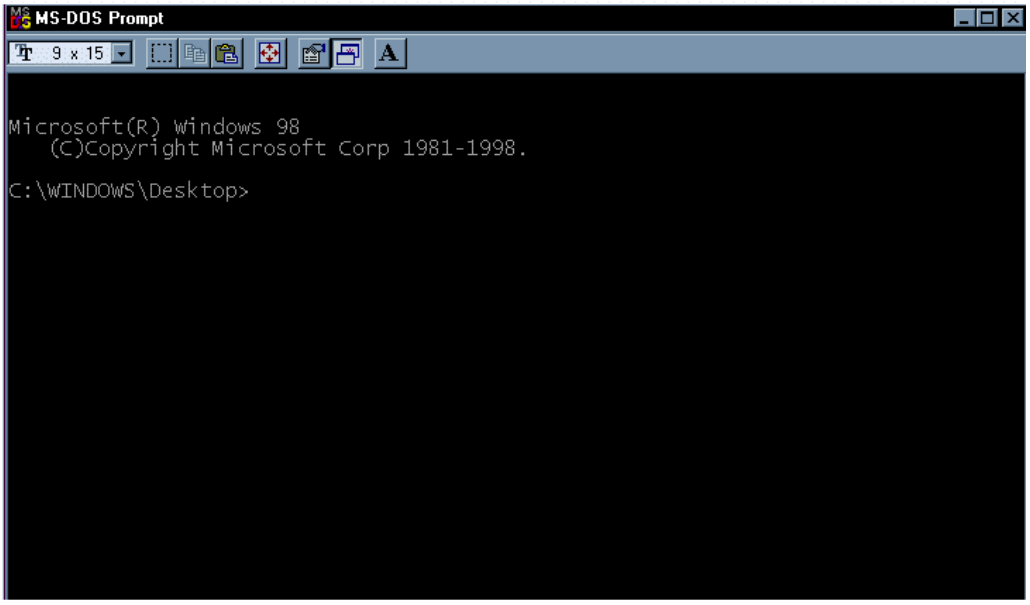
If you use Dial Up Internet Access then you will find your IP address under PPP adapter. If you have dedicated access you will find your IP address under another adapter name like (PCI Busmaster, SMC Adapter, etc.) You can see a list by clicking on the down arrow.



Once you have the IP address write it down, then close that window by clicking (OK) and do the following.

- Click **Start**
- Go to **Run** (Click on **Run**)
- Type command then Click **OK**

At this point you should see a screen that looks like this.



Type the following at the Dos Prompt

- **Nbtstat –A IP address**

For example: nbtstat –A 207.175.1.1

(Please note that you must type the A in capitol letters.)

This will give you a read out that looks like this

NetBIOS Remote Machine Name Table

_____

Name	Type	Status
J-1	<00> UNIQUE	Registered
WORK	<00> GROUP	Registered
J-1	<03> UNIQUE	Registered
J-1	<20> UNIQUE	Registered
WORK	<1E> GROUP	Registered
WORK	<1D> UNIQUE	Registered
__MSBROWSE__.<01>GROUP		Registered

(Again info has been omitted due to privacy reasons)

The numbers in the **<>** are hex code values. What we are interested in is the "Hex Code" number of <20>. If you do not see a hex code of <20> in the list that's a good thing. If you do have a hex code <20> then you may have cause for concern. Now you're probably confused about this so I'll explain.

A hex code of <20> means you have file and printer sharing turned on. This is how a "hacker" would check to see if you have "file and printer sharing" turned on. If he/she becomes aware of the fact that you do have "file and printer sharing" turned on then they would proceed to attempt to gain access to your system.

(Note: To exit out of the DOS prompt Window, Type Exit and hit Enter)

I'll show you now how that information can be used to gain access to your system.

A potential hacker would do a scan on a range of IP address for systems with "File and Printer Sharing" turned on. Once they have encountered a system with sharing turned on the next step would be to find out what is being shared.

This is how:

Net view \\<insert ip_address here>

Our potential hacker would then get a response that looks something like this.

Shared resources at \\ip_address

Sharename	Type	Comment
MY DOCUMENTS	Disk	
TEMP	Disk	

The command was completed successfully.

This shows the hacker that his potential victim has their My Documents Folder shared and their Temp directory shared. For the hacker to then get access to those folders his next command will be.

Net use x: \\<insert IP address here>\temp

If all goes well for the hacker, he/she will then get a response of

(The command was completed successfully.)

At this point the hacker now has access to the TEMP directory of his victim.

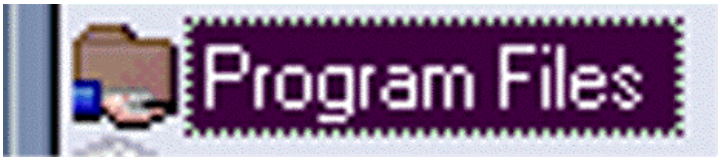
Q. The approximate time it takes for the average hacker to do this attack?

R. 15 seconds or less.

Not a lot of time to gain access to your machine is it? How many of you had “File and Printer Sharing” turned on?

Ladies and Gentlemen: This is called a Netbios attack. If you are running a home network then the chances are you have file and printer sharing turned on. This may not be the case for all of you but I’m sure there is quite a number of you who probably do. If you are sharing resources please password protect the directories.

Any shared directory you have on your system within your network will have a hand holding the folder. Which looks like this.



You can check to find which folders are shared through Windows Explorer.

- Click On Start
- Scroll Up to Programs

At this point you will see a listing of all the different programs on your system

Find Windows Explorer and look for any folders that look like the above picture.

Once you have found those folders password protect them. Don’t worry I’ll show you how to accomplish this in Chapter 8 in a visual step by step instruction format.

Netbios is one of the older forms of system attacks that occur. It is usually overlooked because most systems are protected against it. Recently there has been an increase of Netbios Attacks.

Further on in this manual we shall cover some prevention methods. For now I wish only to show you the potential security flaws.

Chapter

2

THE TROJAN “HORSE”

I found it necessary to devote a chapter to Trojans. Trojan’s are probably the most compromising of all types of attacks. Trojans are being released by the hundreds every week, each more cleverly designed that the other. We all know the story of the Trojan horse probably the greatest strategic move ever made.

In my studies I have found that Trojans are primarily responsible for almost all Windows Based machines being compromised.

For those of you who do not know what Trojans are I’ll briefly explain. Trojans are small programs that effectively give “hackers” remote control over your entire Computer.

Some common features with Trojans are as follows:

- Open your CD-Rom drive
- Capture a screenshot of your computer
- Record your key strokes and send them to the “Hacker”
- Full Access to all your drives and files
- Ability to use your computer as a bridge to do other hacking related activities.
- Disable your keyboard
- Disable your mouse…and more!

Let’s take a closer look at a couple of more popular Trojans:

- Netbus
- SubSeven

The Netbus Trojan has two parts to it as almost all Trojans do. There is a Client and a Server. The server is the file that would have to get installed on your system in order to have your system compromised. Here’s how the hack would go.

The Hack

Objective: Getting the potential victim to install the server onto his/her system.

Method 1

Send the server file (for explanation purposes we'll call the file netbusserver.exe) to you via E-Mail. This was how it was originally done.

The hacker would claim the file to be a game of some sort. When you then double click on the file, the result is nothing. You don't see anything. **(Very Suspicious)**

Note: (How many times have you double clicked on a file someone has sent you and it apparently did nothing)

At this point what has happened is the server has now been installed on your system. All the "hacker" has to do is use the Netbus Client to connect to your system and everything you have on your system is now accessible to this "hacker."

With increasing awareness of the use of Trojans, “hackers” became smarter, hence method 2.

Method 2

Objective: Getting you to install the server on your system.

Let’s see, how many of you receive games from friends? Games like hit gates in the face with a pie. Perhaps the game shoot Saddam? There are lots of funny little files like that. Now I’ll show you how someone intent on getting access to your computer can use that against you.

There are utility programs available that can combine the (“server” (a.k.a. Trojan)) file with a legitimate “executable file.” (An executable file is any file ending in .exe). It will then output another (.exe) file of some kind. Think of this process as mixing poison in a drink.

For Example:

Tomato Juice + Poison = something

Now the result is not really Tomato Juice anymore but you can call it whatever you want. Same procedure goes for combining the Trojan with another file.

For Example:

The “Hacker” in question would do this: (for demonstration purposes we’ll use a chess game)

Name: chess.exe (name of file that starts the chess game)

Trojan: netbusserver.exe (The Trojan)

(Again for explanation purposes we’ll call it that)

The joiner utility will combine the two files together and output 1 executable file called:

<insert name here>.exe

This file can then be renamed back to chess.exe. It's not exactly the same Chess Game. It's like the Tomato Juice, it's just slightly different.

The difference in these files will be noticed in their size.

The original file: chess.exe size: 50,000 bytes

The new file (with Trojan): chess.exe size: 65,000 bytes

(Note: These numbers and figures are just for explanation purposes only)

The process of joining the two files, takes about 10 seconds to get done. Now the "hacker" has a new chess file to send out with the Trojan in it.

Q. What happens when you click on the new chess.exe file?

Answer: The chess program starts like normal. No more suspicion because the file did something. The only difference is while the chess program starts the Trojan also gets installed on your system.

Now you receive an email with the attachment except in the format of chess.exe.

The unsuspecting will execute the file and see a chess game. Meanwhile in the background the "Trojan" gets silently installed on your computer.

If that's not scary enough, after the Trojan installs itself on your computer, it will then send a message from your computer to the hacker telling him the following information.

Username: (A name they call you)

IP Address: (Your IP address)

Online: (Your victim is online)

So it doesn't matter if you are on dial up. The potential hacker will automatically be notified when you log on to your computer.

You're probably asking yourself "how likely is it that this has happened to me?" Well think about this. Take into consideration the second chapter of this manual. Used in conjunction with the above mentioned methods can make for a deadly combination.

These methods are just but a few ways that "hackers" can gain access to your machine.

Listed below are some other ways they can get the infected file to you.

News Groups:

By posting articles in newsgroups with file attachments like (mypic.exe) in adult newsgroups are almost guaranteed to have someone fall victim.

Don't be fooled though, as these folks will post these files to any newsgroups.

Grapevine:

Unfortunately there is no way to control this effect. You receive the file from a friend who received it from a friend etc. etc.

Email:

The most widely used delivery method. It can be sent as an attachment in an email addressed to you.

Unsafe Web sites:

Web sites that are not “above the table” so to speak. Files downloaded from such places should always be accepted with high suspicion.

IRC:

On IRC servers sometimes when you join a channel you will automatically get sent a file like “mypic.exe” or “sexy.exe” or sexy.jpg.vbs something to that effect. Usually you’ll find wannabe’s are at fault for this.

Chat Sites:

Chat sites are probably one of the primary places that this sort of activity takes place. The sad part to that is 80% are not aware of it.

As you can see there are many different ways to deliver that file to you as a user. By informing you of these methods I hope I have made you more aware of the potential dangers around you. In Chapter 3 we’ll discuss what files should be considered acceptable.

Chapter

3

ACCEPTABLE FILES

From the last chapter you're probably asking yourself what exactly is safe to accept as a file from anyone. Hopefully I'll answer most if not all your questions about what types of files can be considered safe or more to the point normal.

I'll show you what normal extensions should be for different types of files and what type of files should never come in .exe formats.

We'll start with something I'm sure most if not all folks have had happen to them at least once.

PICTURES

Ever had someone send you a picture of themselves? If you hang around on a chat site of any kind then chances are you've met someone or a group of people perhaps who've wanted to send you their picture. If they did then hopefully it was not in the form of **(mypic.exe)**. If it was you may want to run a virus check on those files in particular.

For all intensive purposes pictures should really only come in the formats listed below.

- Jpg (jpeg) For example (steve.jpg)
- Bmp (bitmap) For example (steve.bmp)
- TIFF (Tag Image File Format) For example (steve.tiff)
- Gif (Graphics Interchange Format) For example (steve.gif)

These are all legitimate!

Your browser can view almost all of these files short of the tiff format. Other programs that can be used to view these files are Photoshop, Paintshop, Netscape, Internet Explorer and Imaging just to name a few.

WARNING!

These are the file types by which images should come as. Anything else should be unacceptable. There is no reason to have an Image of any kind come as a .exe file. Don't ever accept the excuse that it's an auto extracting image file!

READ ME AND TEXT FILES

Almost all program information documents on the net come in one of these formats. These files are simply information documents typed up in some word processing program or text editor.

Some examples of their extensions are:

- DOC Document format for Microsoft Word, Word. Example: (readme.doc)
- TXT Text format file can be opened by Notepad, Word, Microsoft Word. Example: (readme.txt)
- RTF (Rich Text Format)

Those are all acceptable legitimate formats. The truth is that a text files can come in almost any format. However there are formats that they really should never come in.

For Example:

- <anything>.com
- <anything>.exe
- <anything>.txt.vbs

There is no reason for any files to be sent to you in any of the above formats if they are text documents. I can also assure you there is no reason a file should have a double extension. Such files if you should ever receive them should be treated with suspicion.

By no means should you ever open a file if you do not know what type of file it is.

If you are uncertain about what a file type is here is a method by which you can check. Go to your favorite search engine for example:

Altavista: http://www.altavista.com

Or

Metacrawler: http://www.metacrawler.com

- Click into the search field

(Then type the file type you are inquiring about for example)

- Doc file type
- Exe file type
- Rtf file type

This will pull up sites that will give a more detailed explanation of exactly what type of file it is.

You can use the above information to better understand what type of files you receive from individuals. Without risking installing anything on your machine.

We've covered methods by which your computer can be accessed by a Netbios Attack, how files can be infected, and how they can be delivered. In Chapter 4 we'll discuss who is responsible for these attacks. We will look at the type of individuals behind the keyboard responsible for these attacks.

Chapter

4

WHO ARE HACKERS?

I feel it is necessary to clarify the term hacker. Perhaps your definition of a hacker has been influenced and tainted over the years. There have been various computer related activities attributed to the term “hacker”, but were greatly misunderstood. Unfortunately for the people who are truly defined within the underground tech world as a “hacker” this is an insult to them.

There are various types of “hackers”, each with their own agenda. My goal is to help protect you from the worst of them.

Anarchist Hackers

These are the individuals who you should be weary of. Their sole intent on system infiltration is to cause damage or use information to create havoc. They are primarily the individuals who are responsible for the majority of system attacks against home users. They are more likely to be interested in what lies on another person’s machine for example yours.

Mostly you’ll find that these individuals have slightly above computer skill level and consider themselves hackers. They glorify themselves on the accomplishments of others. Their idea

of classing themselves as a hacker is that of acquire programs and utilities readily available on the net, use these programs with no real knowledge of how these applications work and if they manage to "break" into someone's system class themselves as a hacker. These individuals are called "Kiddie Hackers."

They use these programs given to them in a malicious fashion on anyone they can infect. They have no real purpose to what they are doing except the fact of saying "Yeah! I broke into <insert name here> computer!" It gives them bragging rights to their friends.

If there is any damage to occur in a system being broken into these individuals will accomplish it.

These individuals are usually high school students. They brag about their accomplishments to their friends and try to build an image of being hackers.

Hackers

A hacker by definition believes in access to free information. They are usually very intelligent people who could care very little about what you have on your system. Their thrill comes from system infiltration for information reasons. Hackers unlike "crackers and anarchist" know being able to break system security doesn't make you a hacker any more than adding 2+2 makes you a mathematician. Unfortunately, many journalists and writers have been fooled into using the word 'hacker." They have attributed any computer related illegal activities to the term "hacker."

Real hackers target mainly government institution. They believe important information can be found within government institutions. To them the risk is worth it. The higher the security the better the challenge. The better the challenge the better they need to be. Who's the best keyboard cowboy? So to speak!

These individuals come in a variety of age classes. They range from High School students to University Grads. They are quite

adept at programming and are smart enough to stay out of the spotlight.

They don't particularly care about bragging about their accomplishments as it exposes them to suspicion. They prefer to work from behind the scenes and preserve their anonymity.

Not all hackers are loners, often you'll find they have a very tight circle of associates, but still there is a level of anonymity between them. An associate of mine once said to me "if they say they are a hacker, then they're not!"

Crackers

For definition purposes I have included this term. This is primarily the term given to individuals who are skilled at the art of bypassing software copyright protection. They are usually highly skilled in programming languages.

They are often confused with Hackers. As you can see they are similar in their agenda. They both fight security of some kind, but they are completely different "animals."

Being able to attribute your attacks to the right type of attacker is very important. By identifying your attacker to be either an Anarchist Hacker or a Hacker you get a better idea of what you're up against.

"Know your enemy and know yourself and you will always be victorious…"

Chapter

5

TOOLS OF THE TRADE

What is a carpenter without a hammer? “Hackers” require tools in order to attempt to compromise a systems security. Some tools are readily available and some are actually written by other hackers, with the sole intent of being used for system break-ins. Some “hackers’ use a little ingenuity with their attacks and don’t necessarily rely on any particular tool. In the end however it boils down to they need to infect your system in order to compromise it.

To better understand the means by which “hackers” compromise system security I feel it important to understand what tools they use. This will give you as a user insight as to what exactly they look for and how they obtain this information. In this section, I also explain how these tools are used in conjunction with each other.

Port Scanners

What is a port scanner?

A port scanner is a handy tool that scans a computer looking for active ports. With this utility, a potential “hacker” can figure out what services are available on a targeted computer from the responses the port scanner receives. Take a look at the list below for reference.

Starting Scan.

Target Host: www.yourcompany.com

TCP	Port	:7	(echo)
TCP	Port	:9	(discard)
TCP	Port	:13	(daytime)
TCP	Port	:19	(chargen)
TCP	Port	:21	(ftp)
TCP	Port	:23	(telnet)
TCP	Port	:25	(smtp)
TCP	Port	:37	(time)
TCP	Port	:53	(domain)
TCP	Port	:79	(finger)
TCP	Port	:80	(www)
TCP	Port	:110	(pop)
TCP	Port	:111	(sunrpc)

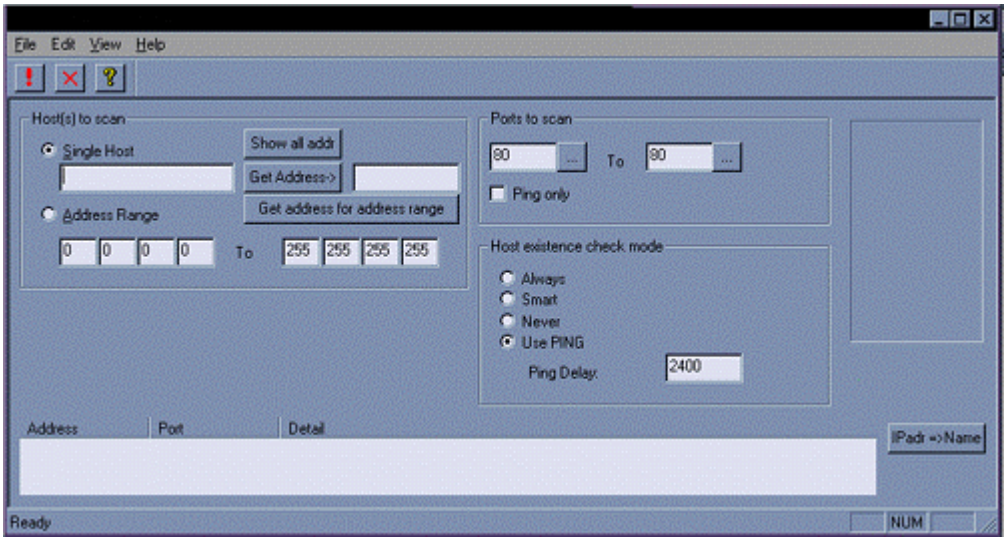
Finished.

Scanning for open ports is done in two ways. The first is to scan a single IP address for open ports. The second is to scan a range of IP address to find open ports.

Try to think about this like calling a single phone-number of say 555-4321 and asking for every extension available. In relation to scanning, the phone-number is equivalent to the IP address and the extensions to open ports.

Scanning a range of IP address is like calling every number between 555-0000 to 555-9999 and asking for every extension available at every number.

Q. What does a port scanner look like?



Trojans

Trojans are definitely one of the tools that “hackers” use. There are hundreds of Trojans. To list them all would make this manual extremely long. For definition purposes we’ll focus on a couple.

Sub Seven

The Sub Seven Trojan has many features and capabilities. It is in my opinion by far the most advance Trojan I have seen. Take a look at some of the features of Sub Seven.

- address book
- WWP Pager Retriever
- UIN2IP
- remote IP scanner
- host lookup
- get Windows CD-KEY
- update victim from URL
- ICQ takeover
- FTP root folder
- retrieve dial-up passwords along with phone numbers and usernames
- port redirect
- IRC bot. for a list of commands
- File Manager bookmarks
- make folder, delete folder [empty or full]
- process manager
- text 2 speech
- Restart server
- Aol Instant Messenger Spy
- Yahoo Messenger Spy
- Microsoft Messenger Spy
- Retrieve list of ICQ uins and passwords
- Retrieve list of AIM users and passwords
- App Redirect
- Edit file
- Perform clicks on victim's desktop
- Set/Change Screen Saver settings [Scrolling Marquee]
- Restart Windows [see below]
- Ping server
- Compress/Decompress files before and after transfers
- The Matrix
- Ultra Fast IP scanner
- IP Tool [Resolve Host names/Ping IP addresses]

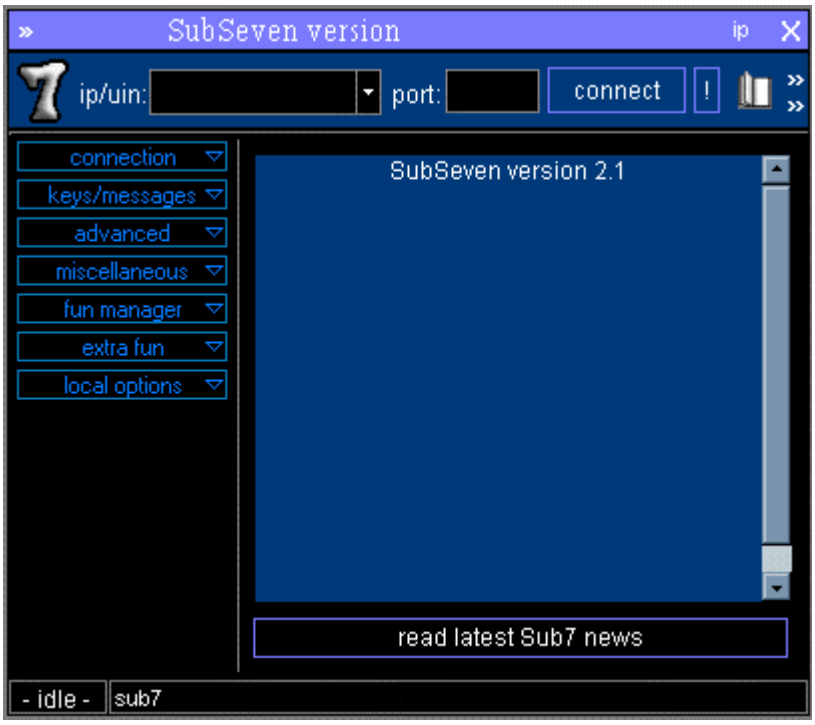
Continued...

- Get victim's home info [not possible on all servers]:

  - Address
  - Bussiness name
  - City
  - Company
  - Country
  - Customer type
  - E-Mail
  - Real name
  - State
  - City code
  - Country code
  - Local Phone
  - Zip code

And more…

I think you get the picture of just exactly what that Trojan is capable of. Here is a picture of what SubSeven looks like.



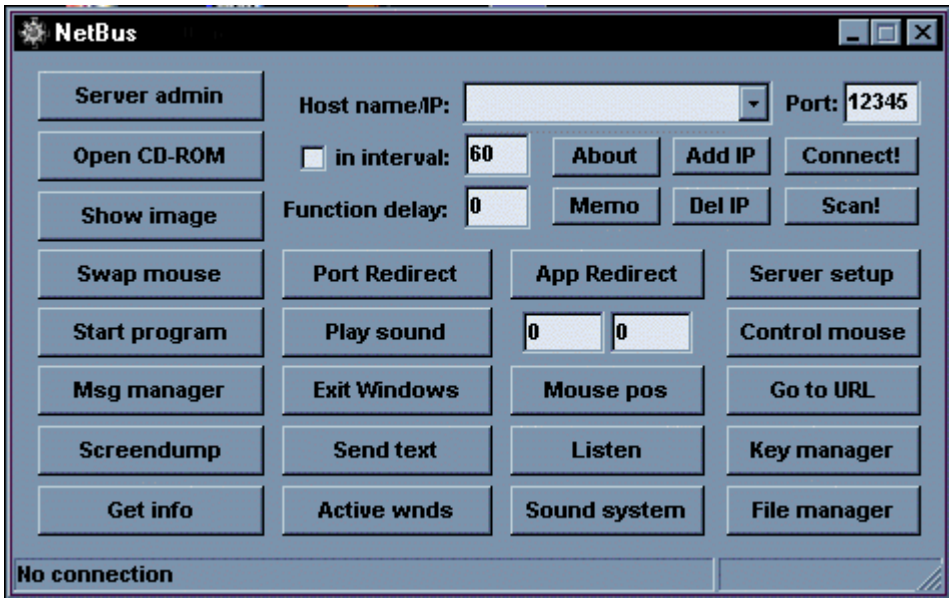
Netbus:

NetBus is an older Trojan however nonetheless is still used. It consists of a server and a client-part. The server-part is the program which must be running on your computer. This should give you an idea of what Netbus is capable of.

Netbus Features:

- Open/close the CD-ROM once or in intervals (specified in seconds).
- Show optional image. If no full path of the image is given it will look for it in the Patch-directory. The supported image-formats is BMP and JPG.
- Swap mouse buttons – the right mouse button gets the left mouse button's functions and vice versa.
- Start optional application.
- Play optional sound-file. If no full path of the sound-file is given it will look for it in the Patch-directory. The supported sound-format is WAV.
- Point the mouse to optional coordinates. You can even navigate the mouse on the target computer with your own.
- Show a message dialog on the screen. The answer is always sent back to you.
- Shutdown the system, logoff the user etc.
- Go to an optional URL within the default web-browser.
- Send keystrokes to the active application on the target computer. The text in the field "Message/text" will be inserted in the application that has focus. ("|" represents enter).
- Listen for keystrokes and send them back to you.
- Get a screendump (should not be used over slow connections).
- Return information about the target computer.
- Upload any file from you to the target computer. With this feature it will be possible to remotely update Patch with a new version.

- Increase and decrease the sound-volume.
- Record sounds that the microphone catch. The sound is sent back to you.
- Make click sounds every time a key is pressed.
- Download and deletion of any file from the target. You choose which file you wish to download/delete in a view that represents the harddisks on the target.
- Keys (letters) on the keyboard can be disabled.
- Password-protection management.
- Show, kill and focus windows on the system.
- Redirect data on a specified TCP-port to another host and port.
- Redirect console applications I/O to a specified TCP-port (telnet the host at the specified port to interact with the application).
- Configure the server-exe with options like TCP-port and mail notification.



This is what the Netbus client looks like.

Joiners

Earlier you saw me make references to utilities that combine two executable files into one. That's what these programs are. These programs make it possible to hide the Trojans in legitimate files.

ICQ

Though as itself is not a utility for hacking there are program files written by Un-named programmers for it. The more advance Trojans have the ability to notify the "hacker" via ICQ of whether or not you are online. Given that you are infected with a Trojan.

If you are not infected then ICQ can serve as a Utility to give away your IP address. Currently there are files/programs available on the net that allows you to "patch" ICQ so it reveals the IP numbers of anyone on the "hackers" list. There are also files that allow you add users in ICQ without their authorization or notification.

For demonstration purposes let's see how a hack would go if a hacker with the above mentioned utilities were to attempt to hack into a users machine.

Hack 1:

Objective: Obtain entry to the users machine.

Step1: Obtain user's ICQ #
Step2: Add User to ICQ list
Step3: Use Get Info on user
Step4: Record User's IP address
Step5: Start a dos prompt
Step6: nbtstat –A <ipaddress>
Step7: Look for hex code <20>
Step8: (Assuming a hex of <20> is there) net view \\ip_address.
Step9: See what shares are available we'll say "C" is being shared.
Step10: net use x: \\ip_address\c

Access to the user's machine has been achieved.

In the above scenario our "potential hacker" used the patch programs available for ICQ to gain the IP address of the "victim" and then launch his assault.

With the realization of how an "individual" can gain access to your machine let's move on to Chapter 6. We will discuss what's at risk once your computer has been compromised.

Chapter

6

ACCESS GRANTED

Quite often I hear comments like “so what if they hack into my system there’s nothing on my system of interest.” I can’t tell you how more wrong you can be. The only thing I can think of when I hear someone say that is that person is not aware of just what type of information they have access to.

I’ll show you exactly what type of information a “hacker” has access to once your system has been broken into. Try to remember this is not meant to scare you, it is meant to inform you. Keep in mind you are reading this manual to gain a better understanding of how to protect your-self.

Bank Account Information

I'm sure if you're like most people you have web banking of some kind. You probably pay your bills online via your banks website. Most banks require you to use 128bit encryption browsers to do your banking online. This form of banking online does encrypt your information and protect it from otherwise prying eyes of the world that may wish to gain access to such vital information.

This should further illustrate how powerful the encryption method is:

- 40-bit encryption, means there are **2^{40} possible keys** that could fit into the **lock** that holds your account information. That means there are many billions (a 1 followed by 12 zeroes) of possible keys.
- 128-bit encryption, means there are **2^{88}** (a three followed by 26 zeroes) times as many key combinations than there are for 40-bit encryption. That means a computer would require exponentially more processing power than for 40-bit encryption to find the correct key.

That's a very powerful method of encrypting data sent from your machine to the banks machine. Unfortunately it's useless to you once your computer has been compromised.

Question: How?

One of the features of a "Trojan" is a key logger. The principle behind this is all keystrokes pressed will be recorded and sent back to the "hacker."

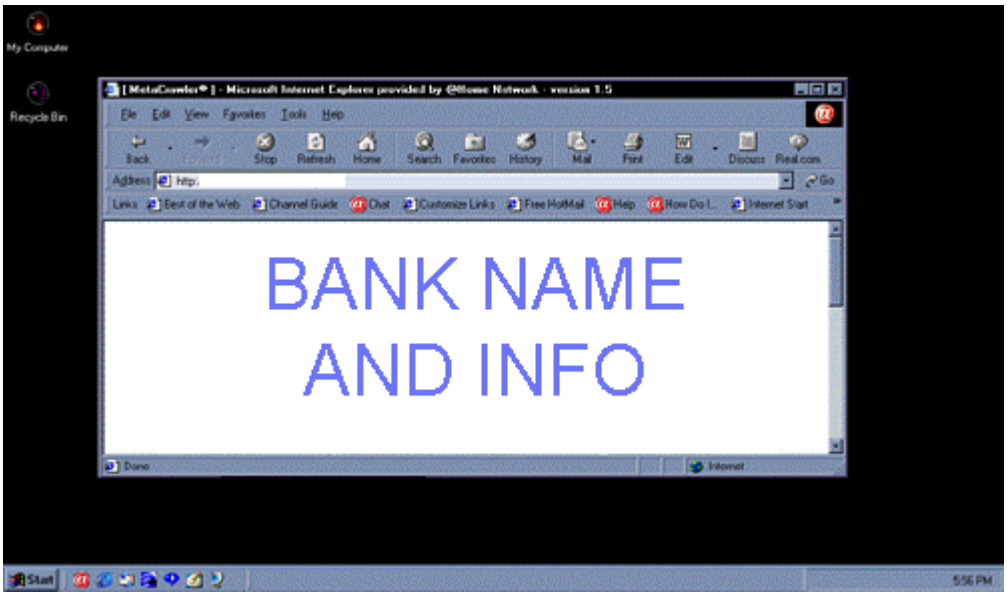
What sort of information do you enter when you are banking online?

Most banks have a login screen of some kind, where you type in your username and password. Here's where it gets interesting.

This means that once you type your login and password for your online bank account the "hacker" now has access to that.

You're probably asking yourself well "How do they know what bank I'm with?"

This information is easily achieved by doing what is called a screen shot. This gives the "hacker" a picture of your desktop and all windows currently open at the time. The screen shot would look like this.



From that screen shot they can tell what site you are at (in which case it would be your bank). From there it's just a matter of logging into your bank account and doing whatever they want.

As you can see although you are on a secure web site, it still doesn't protect your information once your computer is compromised.

Perhaps there are some of you who do not use online banking. Perhaps you use another program for managing your finances. There is a variety of programs out there available for financial purposes.

Problem is that once a "hacker" has access to your system, they have access to those files. They can copy the files from your computer to theirs and browse through them at their leisure.

Email

Simply put all emails sent to you are accessible to a “hacker” once your system has been compromised. They can read them and possibly check your mail before you do.

Pictures

If you have pictures of yourself or family members on your system, they are also available to the “hacker.” I don’t think I need to explain the danger here. Not only has the individual compromised your computer system, they also know what you look like.

Resume

This may not sound like a priority file for a “hacker” but stay with me for a second. How many of you have resumes typed up on your computers? I’m sure a lot of you do. If a “hacker” were to download your resume they now have access to:

Name:
Address:
Phone:
Workplace:

Add to that the above and let’s take a look at what they know.

- Email address of friends, family, associates.
- Your home address.
- Phone Number
- What you look like
- Where you work (And have worked)
- Bank Account (including how much money you have)

It doesn't stop there either. Those are just a few of the things that can happen when your system is compromised. This is no science fiction these are real life possibilities. The extent of that information was gathered just from files on your system. Take into consideration the following.

SURVELLANCE VIA INTERNET CONNECTION

Make no mistake this is very real. Depending on how much you read and how much you know about Trojans you are probably aware of what I am talking about.

If you are not aware, then I am referring to the ability to effectively turn your computer into an audio/video survellance unit without you knowing.

Question: How?

Answer: How many of you have Webcams? How many of you have Microphones?

Not all Trojans have the ability to access your Web Cam and Microphone. The ones that do, have the ability to turn your computer into a video/audio survellance camera.

The Trojan records the sounds in a room via your microphone and then sends the file back to the "hacker." The hacker then plays the file back and can hear any sounds recorded in the room. Add to that since the recording is a file they can play it back whenever they want to who ever they want.

By the same method they access your Web Cam effectively getting both a video and audio feed from your house of what is currently going on in that room.

That sounds crazy, but I can assure you it is not. I don't think I need to tell you what type of security hazard this represents to you and your family.

By now you are probably worried/scared of the possible vulnerabilities of your computer. Don't be. In Chapter 7 we will discuss methods to protect yourself from these individuals.

Chapter

7

HOW TO PROTECT YOURSELF

There is a saying that goes “Prevention is better than cure.” After reading this manual hopefully you are looking for ways to protect your privacy. Take it back from those who may invade it.

The individuals who are responsible for these attacks will always prey off those who do not take an interest in defending their privacy.

“Give a man a fish and he’ll eat for the day. Teach a man how to fish and he’ll never starve.”

By showing you steps and procedures you can use to protect your system from being hacked, you’ll quickly regain your sense of security.

FIREWALLS

A firewall in layman terms is essentially a program which filters network data to decide whether or not to forward them to their destination or to deny it.

These programs will generally protect you from inbound “net attacks.” This means unauthorized network request from foreign computers will be blocked.

I cannot stress how important it is in this day and age to have a firewall of some kind installed and “running” on your computer.

I personally recommend that you use one of the following or both if you can.

Black Ice Defender

This is a very user-friendly comprehensive firewall program. I highly recommend it to both advance and novice users. It has a simple graphical interface that is easy to understand and pleasing to the eye.

It detects your attacker, stops their attack and or scan and gives you as much information available on the “attacker.”

You can download Black Ice Defender at:

http://www.networkice.com

Lockdown 2000

I also recommend Lockdown 2000 as a security measure. Lockdown2000 has a very nice graphical interface to it also and is user friendly. It does the same thing Black Ice Defender does but also runs scans on your system for Trojans. It monitors your registry and system files for changes that occur. Then gives you the option of either undoing all the changes or allowing it.

You can obtain a copy of Lockdown2000 from:

http://www.lockdown2000.com

I find using both firewalls in conjunction with each other works quite well. As they both compensate for the short-comings of the other.

Anti Virus Software

This is also another piece of software you should by all means have on your system. We all know it's a necessity however we are all guilty of not using them.

There are numerous anti-virus software out there. Norton Antivirus and Mcafee are two of the more common ones. They are all good and do their job.

You can find each of these programs at:

http://www.norton.com

http://www.mcafee.com

I personally recommend using 1 virus scanner and both firewalls. The reason is I find Black Ice Defender blocks incoming attacks and any system changes that occur on your system Lockdown catches.

TIPS & TRICKS

I feel it necessary for you to pay particular attention to this section. The above programs will function and do their job, but that's only half the battle.

There are certain precautions you need to take as a user to ensure your system remains a "fortress."

Tip #1:

For Dial Up users: If you are a dial up user then you use a modem either internal or external kind to get online. If you have an external modem then this tip is easy. If you look at the modem you'll see lights on the front of it.

When you're doing anything on the net you'll notice lights blinking that indicate that you are Sending Data, and Receiving Data. Depending on how often the lights blink and how fast they blink gives a rough idea of how much activity is going on between your computer and the net.

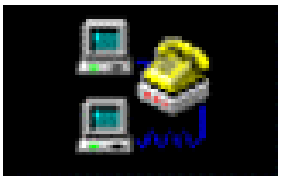
Here's where a little perception comes into play. If you are connected to the internet, and are just sitting by your system doing absolutely nothing, those lights have no business to be blinking rapidly. They will flash periodically indicating it's checking it's connectivity, however there should be no heavy data transfer of any kind if you are not doing anything on the net.

For Example: If you have your email program open and you are just sitting there reading your mail, you may notice that every 15 sometimes 20 mins that the lights will blink back and forth

indicating it's sending and receiving data. This is normal because chances are you have your email program configured to check your mail every 20 mins.

If by chance you notice the lights on your modem is blinking consistently for let's say a period of 2mins non stop be extremely suspicious.

If you have an internal modem, you will not be able to see the lights on your modem, instead you can rely on the two tv looking icons at the bottom right corner of your screen near the clock. They will look something like this.



Any data being sent and received will be noticed by the blinking of the lights rapidly.

If you are on cable or dsl, the same applies. There should never be any form of heavy data transfer of any kind from your system to anything unless you are authorizing it. Some examples of activity that can justify heavy data transfer are as follows:

- Legitimate Programs running that may need to access the net occasionally. (ie, Email programs)
- If you are running an FTP server where people purposely log into your machine to download files you have given them access to.
- If you are downloading files off the internet

Things of that nature will generate a lot of data transfer.

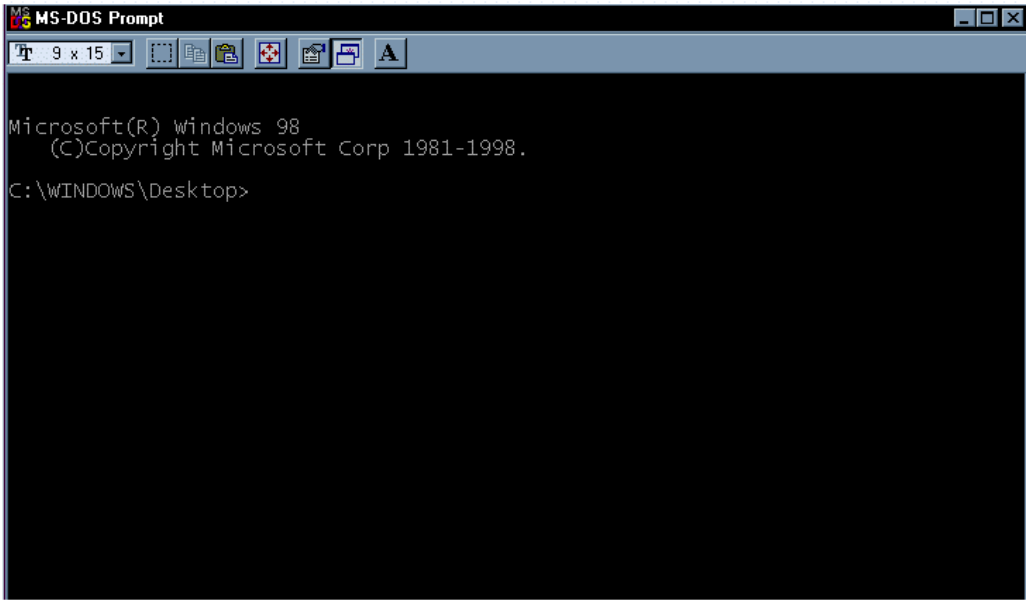
Allow me to take this opportunity to explain to you another “Tool” you should be aware of. Let’s assume you realize that there is a lot of data being sent and received from your machine and you’re not even sitting at it.

How do you know what’s going on?

Let’s do a short exercise.

- Click **Start**
- Go to **Run (Click Run)**
- Type **Command**
- Click **OK**

Again you should get a screen that looks like this.



Once you have this screen type the following:

- **Netstat –a**

This command will give you a listing of everything your computer is communicating with online currently.

The list you get will look something like this:

Active Connections

Protocol	Local Address	Foreign Address	State
TCP	COMP: 0000	10.0.0.1 : 0000	ESTABLISHED
TCP	COMP:2020	10.0.0.5 : 1010	ESTABLISHED
TCP	COMP:9090	10.0.0.3 : 1918	ESTABLISHED

You'll see a variety of listings like the above. It will give you the Protocal being used, the local address (your computer) and what port on your computer the "Foreign Address" is being connected to and the (State) of which the (Foreign Address) is. For example if it is (Established) then that means whatever the foreign address says is currently connected to your machine.

There is software available that will show you this information without typing all those commands.

The name of the software is called Xnetstat, you can obtain a copy of it from here:

http://www.arez.com/fs/xns/

If for whatever reason you believe you are sending and receiving a lot of data then it is wise to do a netstat –a to see what is connected to your computer and at what ports.

Protecting Shared Resources

For those of you who have internal networks between two computers probably have a shared resource of some kind. Earlier in this manual I showed you how to find what is being shared. Let's have a look at how to protect those shared resources.

- Click **Start**
- Scroll up to **Programs**
- Go to **Windows Explorer** (Click on it)

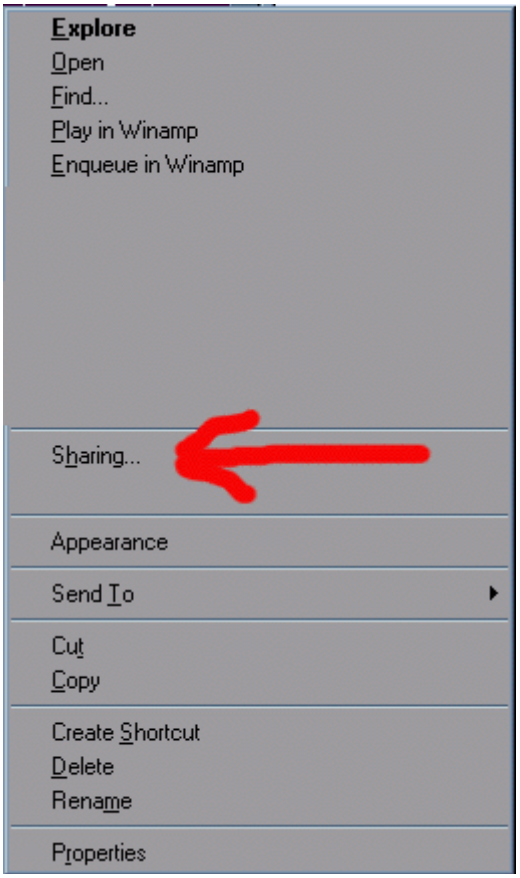
Once you have done this you should see a window that comes up with a bunch of folders listed on the left and more folders listed on the right.

Scroll through the listing and look for whatever shared files you have. For a refresher the folder will look like this.

Once you have found those folders you must now protect them.

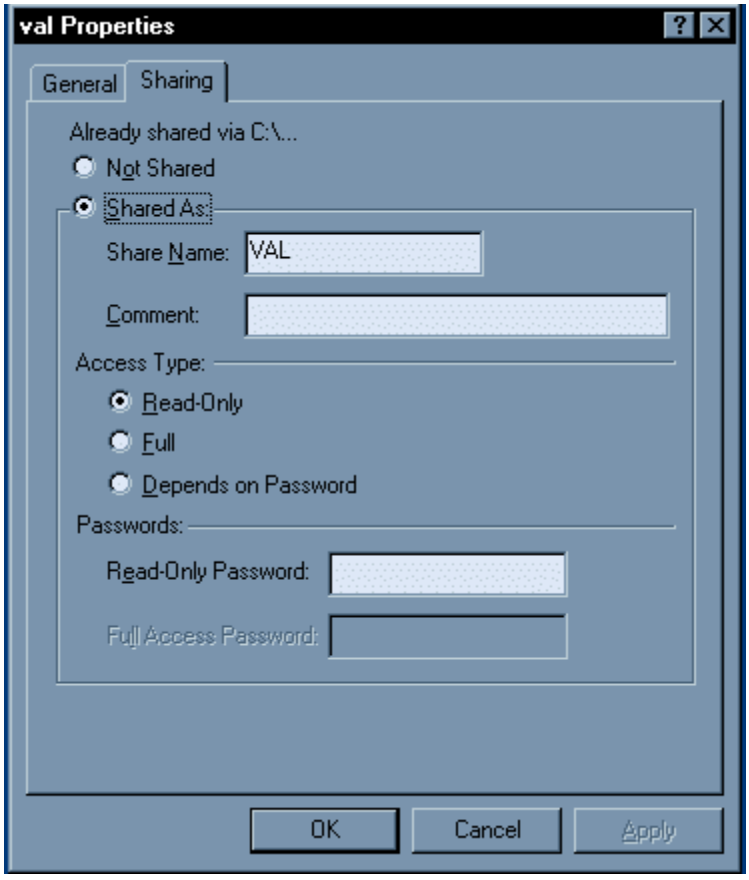
- Click on The folder (once) so it is highlighted
- Use the right mouse button, (the one closest to your pinky finger) and click on the folder.

You will get a menu:

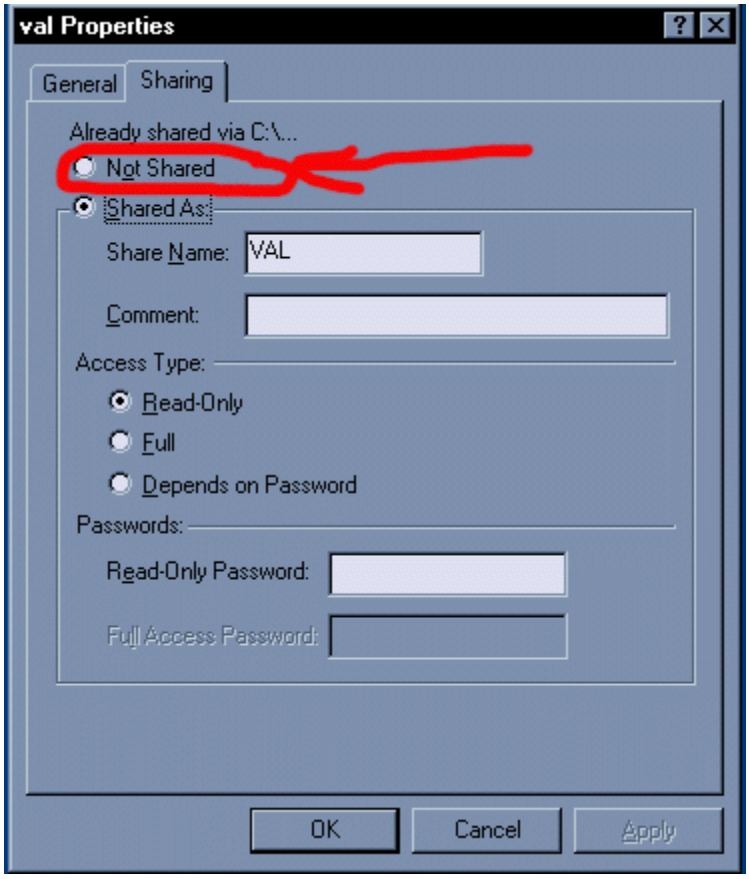


Your menu may look different than mine, but what you're looking for is the word "sharing."

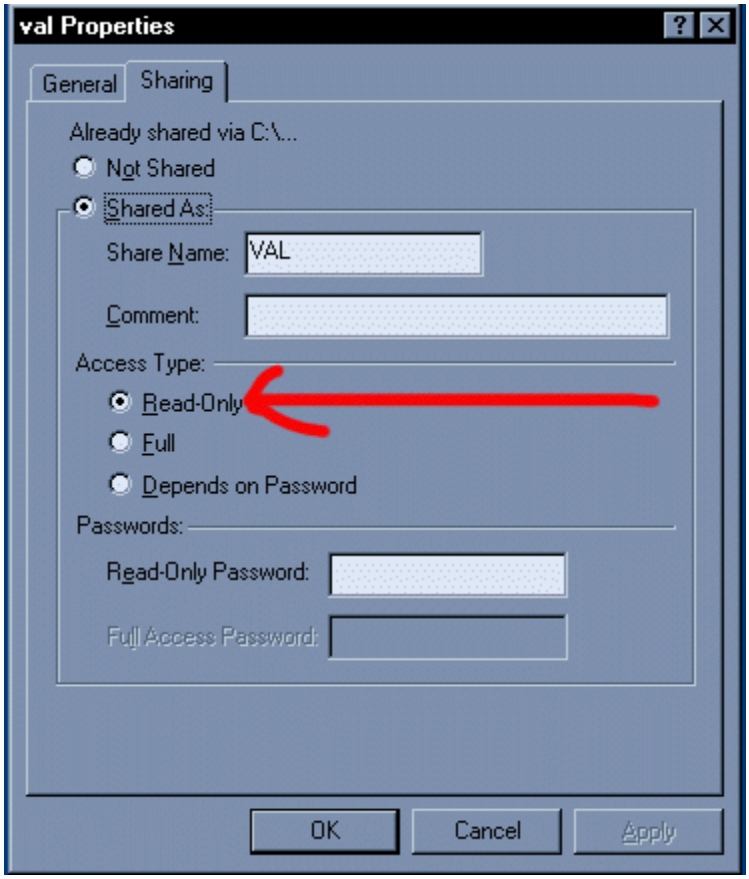
When you click on Sharing you will see another window that looks like the following.



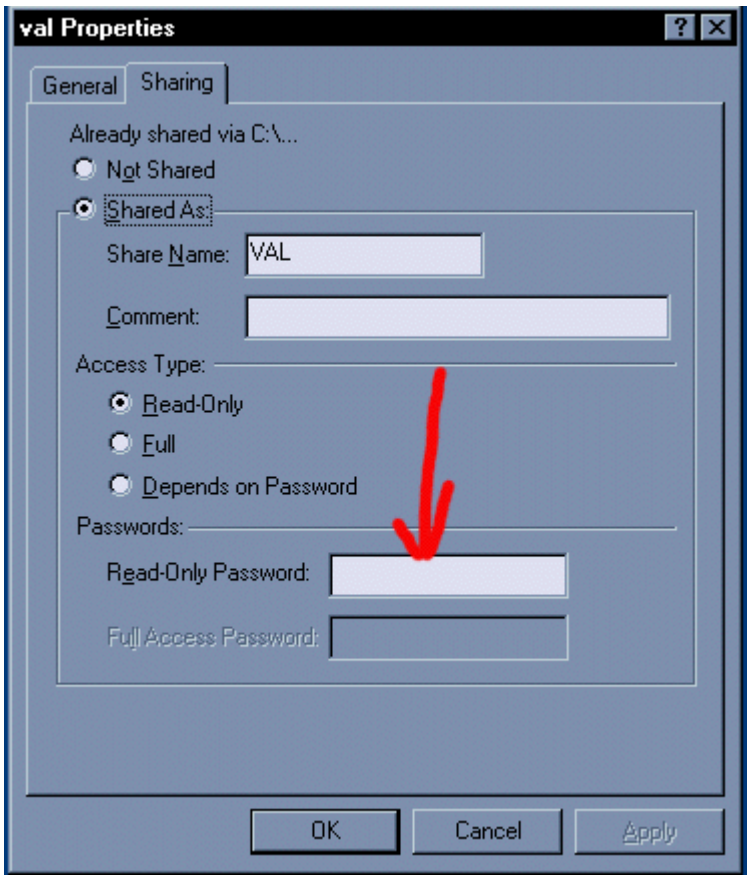
This is where you can either share this folder or turn it off. If you wish to turn off the sharing you would select (Not Shared).



If you must share a folder then follows these steps. This will make the folder read only. That means no one can delete anything from those folders if they were to break into your system using a “Netbios” attack.



The next step is to password protect the directory.



Once you type in the password click (OK) and you're done.

My personal suggestion is to set any directory you are sharing to (Read Only) and password protect it. This is only if you must share resources.

Disabling File and Printer Sharing

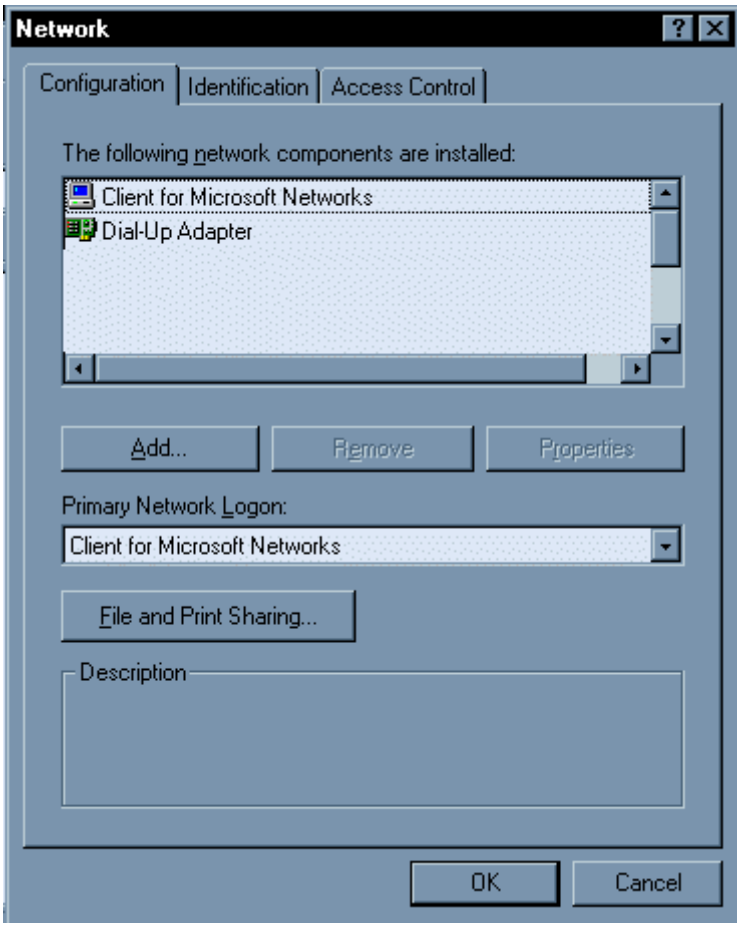
For those of you who do not have a home network going you should disable file and printer sharing. There's no reason to have this feature turned on. Do the following steps to disable it.

(You will require your windows 95/98 CD for this)

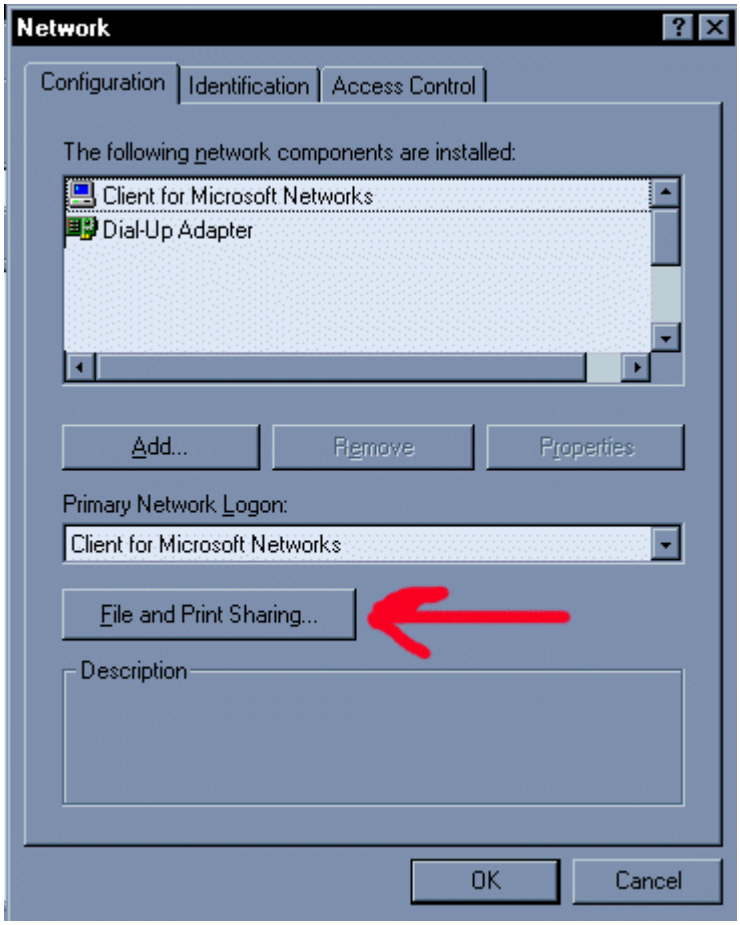
- Click on **Start**
- Scroll up to **Settings**
- Click on **Control Panel**

This will bring you into your Control Panel. You will see a variety of icons the one you are looking for will be the icon that says (Network) and it looks like this.

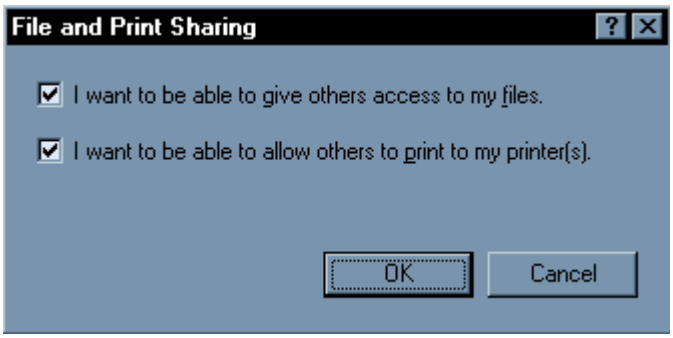
Once you have found the icon double click on it. You will then receive a screen that looks like this.



To turn off the file and printer sharing you will need to click on the button that says (File and Print Sharing).



After clicking on that a box will open:



Uncheck both of these then click okay.

You must then click (OK) again and this will return you to the Control Panel.

At this point will be prompted for you Windows CD. Simply insert it and click OK.

Sometimes you will receive a message that says

“The file being copied is older than the existing file ..etc.etc. Do you wish to keep your existing file?”

You should click NO.

When the process is completely done your system will ask you if you wish to reboot. Click on Yes. Once your system has rebooted you can come back to the Network Screen and check to make sure the “File and Print Sharing” has been disabled.

Software wise up until this point we have talked about how to protect your system. I’d like to discuss the process involved for if you system is infected.

OH NO! MY SYSTEM'S INFECTED

Hope-fully this is not the case for the majority of you, but I know there will be a few people who are going to be infected. The only way you are really going to know if you are infected is diagnosing your computer properly.

I recommend getting **Lockdown 2000** for this. Install it on your system and run a full system scan on your machine. (Consult the documentation for Lockdown 2000)

After running **Lockdown 2000**, run your anti virus scanner just in case **Lockdown** missed anything. You may ask yourself why I suggest such redundancy? Computers are built on the principle of redundancy. One program will always compensate for the short-comings of the other.

This should reveal most if not all Trojans currently residing on your machine. Until you are absolutely sure about not possessing any Trojans on your machine I suggest being alert of the happenings on your computer.

1. Watch the transmit and receive lights on the modem like we discussed.

2. Run the firewall programs I suggested to block out intruders.

3. Monitor your system for unusual happenings (CD Rom opening for no reason)

4. Use the Netstat command to see what ports are being used if you get suspicious.

The ultimate goal is not to be paranoid about the use of your computer. It's about being smart about how you use your computer.

Chapter

8

EVERY SYSTEMS GREATEST FLAW

To every computer system there is always this one system flaw. It does not matter how powerful a system you have, how many different firewall programs you run or how many virus scanners you have. In the end you are your systems worst enemy.

All “hackers” know this, make no mistake about that. Thankfully not very many have the stamina necessary for a form of hacking called “Social Engineering.”

Social Engineering: This is a term used among “hackers” for techniques that rely on weaknesses in people rather than software; the goal is to trick people into revealing passwords or other information that compromises an individual system's security.

This is a lot easier said than done, but it can be done. Most telemarketing scams that rob people of money are forms of “social engineering.” Most of these scams occur due to the individuals impersonating credit card companies and or investment firms. Those socially engineered attacks are focused on getting you to give them your money, bottom line.

Transverse that process into a tech industry where a lot of people are not as computer knowledgeable and you have the “wolf in sheeps clothing!

Some of the most common forms of social engineering focused on any particular user is to phone up a “mark/victim” who has the required information, and posing as a field service tech or a fellow employee with an urgent access problem. This type of attack happens primarily more in business scenes.

Social engineering directed to a business setting usually occur as a phone scam. The scam boils down to how believable the “hacker” sounds on the phone. They pit their knowledge and wits against another human. This technique is used for a lot of things, such as gaining passwords and basic information on a system or organization. Be it known that it’s not the only type of “social engineering” that is used.

These same principles are applied when it comes to your personal computer. Chat lines make people highly susceptible to such social mayhem.

CHATLINE EXAMPLE

On a chat line a person isn’t evaluated by how they appear. They become as believable as their ability to write and express themselves.

On a Chat Line your perception and intuition is all you have to rely on. The person on the other end of the keyboard can be nothing as they describe themselves. The same goes for E-Mail or any form of communication without visual recognition.

You read what they send/say to you and your own imagination is what fills in the blanks. This person may sound romantic, funny and down to earth. There is a trust value that is built up and depending on how long you’ve been on the Internet , this initial base of trust is formed very quickly.

At this point after the ice has been broken so to speak the "hacker" may ask if you wish to see his/her picture. This is the turning point of your conversation. Most people would reply sure and then receive the picture from the "hacker."

This is where the situation gets interesting. The "hacker" in question has the window of opportunity to either attempt to send you a real picture or a Trojan.

If the "hacker" sends you a legitimate picture, then that helps to build trust between them and you. If they go for the strike right of the bat then they risk exposing themselves. In either case their goal has been accomplished which is to get you to accept the file from them.

By gaining your trust and getting you as a user to drop your guard you've compromised your systems security.

Given it takes a certain level of finesse and grace to accomplish this type of attack. It requires the "hacker" to be socially adept, quick witted and very confident. Not usually the characteristics of the stereotypical "hacker" definition.

To protect yourself on this level you must become aware of the "game." The truth is that this is all a game to "hackers." Hackers treasure their anonymity to win against them the trick is to reverse the situation. Get them to expose themselves and their intent.

Let's take a real life situation that you may encounter.

For simplicity sake we'll say you have encountered a "potential hacker" on a chat line. The person seems charming, funny even normal by every sense of the word. The conversation becomes a little personal at some point and while not giving him your life story you share some fairly confidential information with this person.

The conversation heats up and turns to the point of a possible picture trade. The "potential hacker" wishes to trade pictures with you. You tell him/her you don't have a picture and their

remark is something to the effect of “well would you like to see my picture anyway?” So you agree for him/her to send you their picture.

Upon receiving their picture you notice the file is called:

- John.exe or susan.exe

(Recalling what you’ve read in this manual you know that their picture should never be in this format. So you don’t double click on it)

This is where your awareness and intuition kicks in. You have two options.

A) Confront the “potential hacker” about the file type.

B) Play up to the game and see if you can catch this person by making them expose themselves.

If you confront the person perhaps you’ll receive explanations like “it’s a self extracting picture.” At which point you can tell them they are lying. You will probably scare off the “potential hacker” by being that direct with them. They will more than likely log offline very quickly. If you play up to the game you have the chance to maybe catch them, or at least find out who they are.

IRC EXAMPLE

IRC is a hunting ground for “hackers.” It doesn’t take much skill or much know-how, to infect an individuals computer on IRC. Some of the most common tactics is to assume the identity of a girl and going to channels where pictures are commonly exchanged. Channels such as “adults 30+” or “adult-chat.” Hackers know that hacking is 60% psychological warfare 40% computer knowledge.

One of the most popular methods of sending a person a Trojan on IRC is to automatically send you the file when you join a channel. The reason goes as such that some people have a feature turned on in their IRC programs that automatically accepts incoming file transfers.

(Consult your IRC program documentation)

When you join the channel, you automatically accept the file. If you are aware of the file you might see it is called something like **tiffany.jpg.exe.** Out of sheer curiosity some people will open the file to see what it is, especially those who are not aware of the potential dangers of such files. The result is (MISSION ACCOMPLISHED).

As you can clearly see “hackers” are quite adept at the art of subterfuge. They are smart, cunning and do not discriminate against who’s computer they will attempt to gain access too. They will attack whoever falls prey to whatever trap they layout. IRC remains one of the primary sources of victims for “kiddie hackers.”

The recipe for protect yourself requires you to be alert, suspicious and a little paranoia helps. Face it everyone is paranoid about something or the other. In the next chapter we’ll discuss how to go about reporting “hackers.”

Chapter

9

HOW TO REPORT HACKERS

Stopping hackers can be very difficult sometimes seemingly impossible. I believe however if you use the right types of programs combined with self-education on how hackers think, you can make your computer much safer.

Reporting hackers can sometimes be a little bit tricky. A lot of users never report hack attempts. Simply because they just don't care or believe that the "hacker" knows he can't get into their system. There is also the reason that users just don't know what steps to take once they realize their system is being attacked.

Once your system is connected to the Internet, some form of system attack will eventually hit your computer. Most of the times these attacks will be completely random. While not every single attack ever made should be reported, repetitious attacks should. Repeated attacks from the same person/IP address should always be reported. This is a clear indication that someone is trying to gain access to your computer.

If you are using Black Ice Defender and or Lockdown 2000, you will be able to see the IP address of the person attempting to break into your system.

What do you do now that you know that someone is attempting to hack into your computer?

Before you can do anything you will require some utilities. I recommend getting the following program.

- NetLab

Netlab has a variety of utilities combined into one easy to use application.

You can obtain a copy of Netlab from:

http://www.filedudes.lvdi.net/win95/dns/netlab95.html

After obtaining a copy of NetLab and installing it you'll be ready. I find the best procedure for this is to begin by identifying how many times this "individual" has attempted to hack into your system, and at what times.

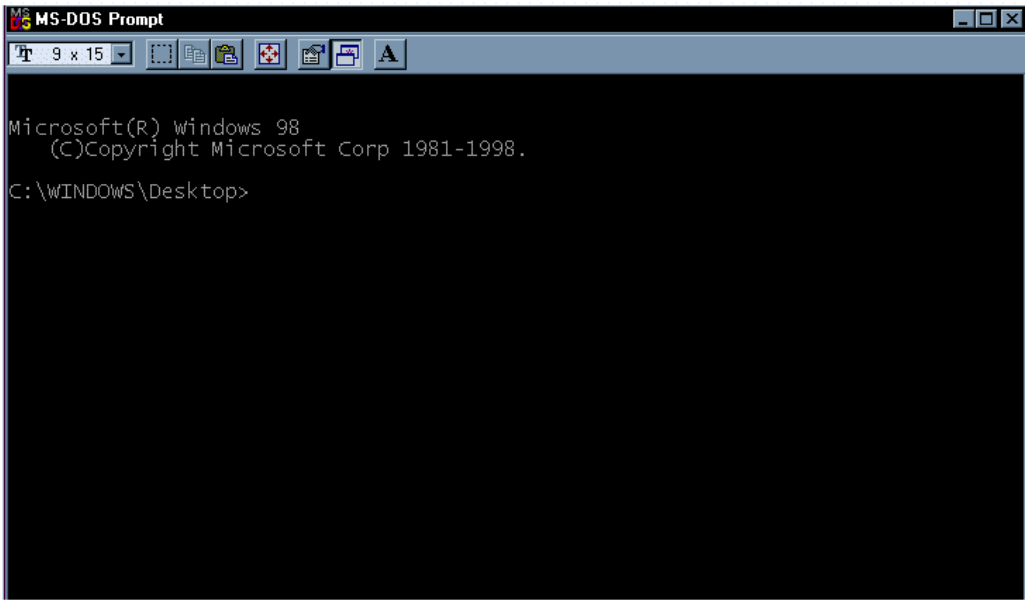
(Consult your firewall program documentation for instructions on where to locate the number of attacks originating from an IP address.)

Once you have identified how many times the person has attempted to gain access and at what time the most recent attack was, it is a wise idea to check if they actually got through.

To check what is currently connected to your computer, do the following:

- Write down the IP address you were given by Black Ice and or Lockdown 2000
- Click **Start**
- Go to **Run**
- Type in **Command** and hit E**nter**

This will bring you to your DOS prompt again.



Type the following at the DOS prompt.

- **Netstat**

This will give you a listing of all active connections to your computer and it will look something like this.

Active Connections

Protocol	Local Address	Foreign Address	State
TCP	COMP: 0000	10.0.0.1 : 0000	ESTABLISHED
TCP	COMP:2020	10.0.0.5 : 1010	ESTABLISHED
TCP	COMP:9090	10.0.0.3 : 1918	ESTABLISHED

Your information will have different numbers. I used the IP address 10.0.0.x for demonstration purposes only.

If your attacker is connected to your computer, you will see his IP address in this listing. Compare this listing to the IP address you have written down.

In the table above you will see numbers after a (:)

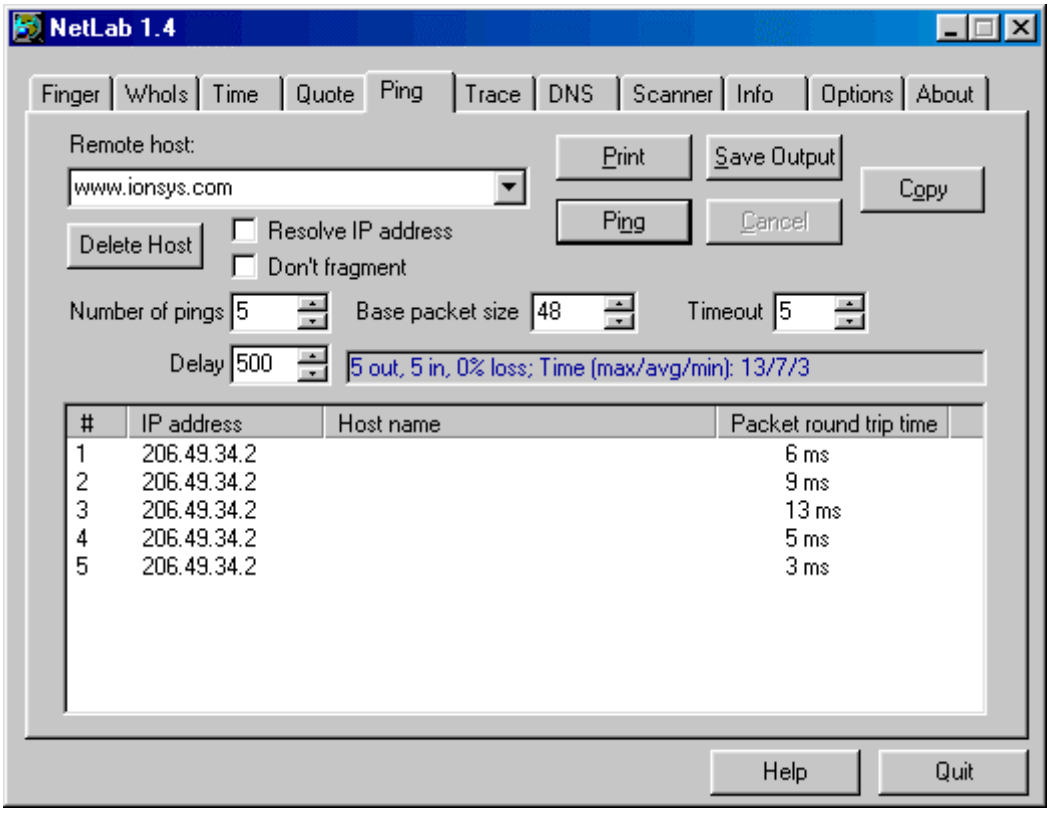
For example: COMP: 2020

The 2020 represents the port number that the Foreign computer is connected to on your computer.

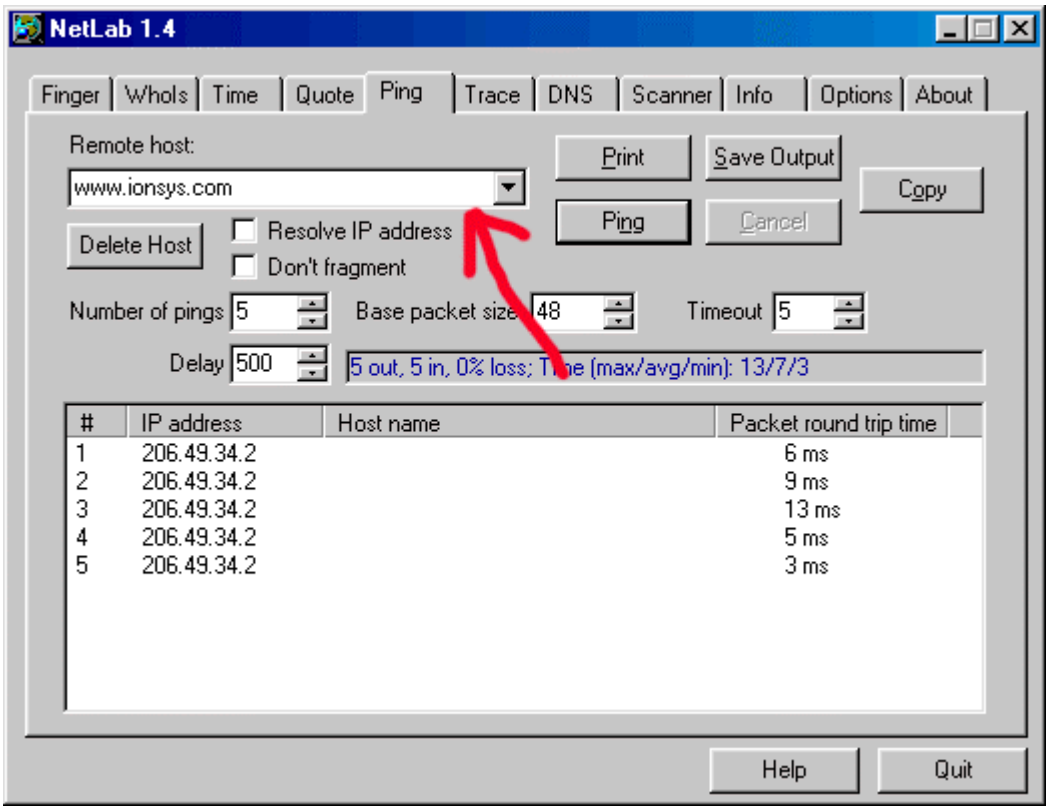
Using our example let's take a look at the second row. This shows us that someone is connected to our computer on port (2020) from the IP address 10.0.0.5.

Once you have assessed that the "hacker" was unsuccessful in his attempts to hack into your computer, you can proceed to gather information to report the attack.

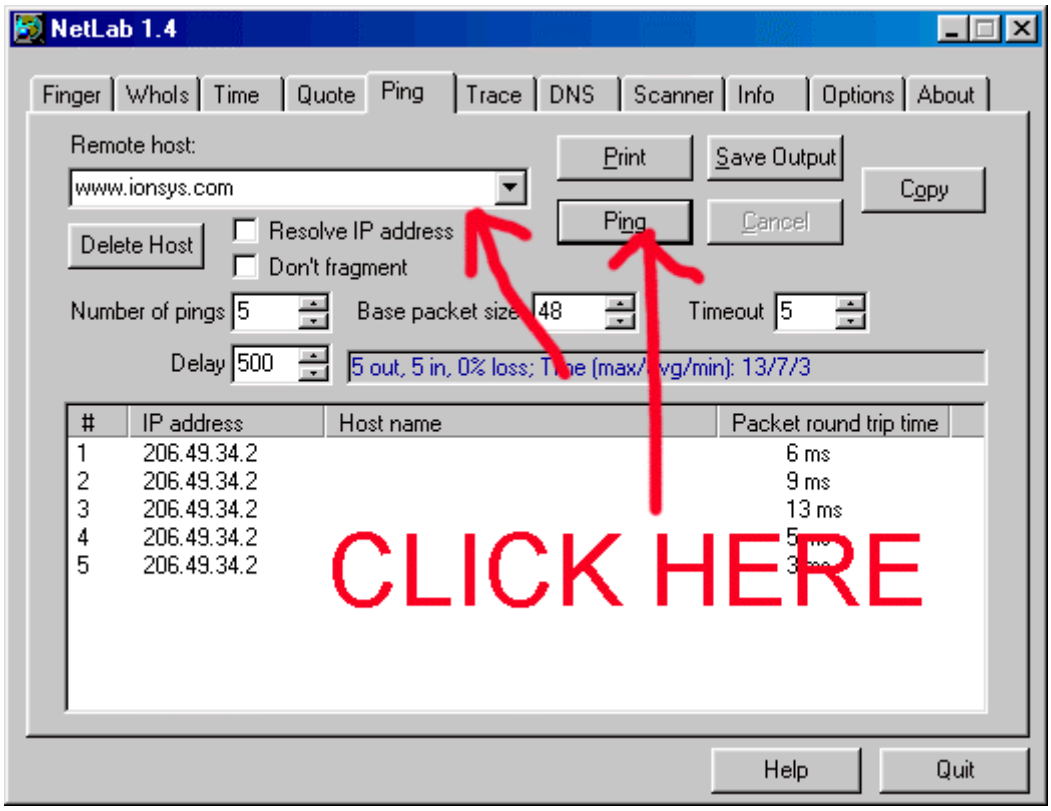
Start up NetLab



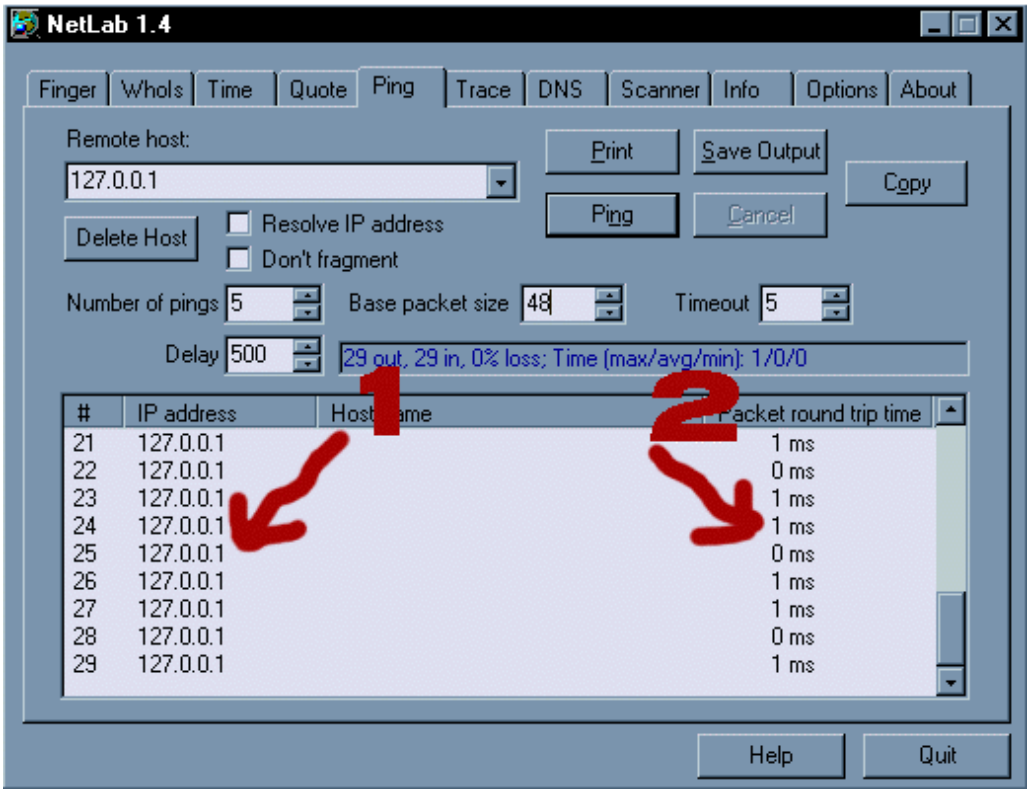
- Type in the IP Address in the indicated area below



- After typing in the IP Address Click on **Ping** indicated below



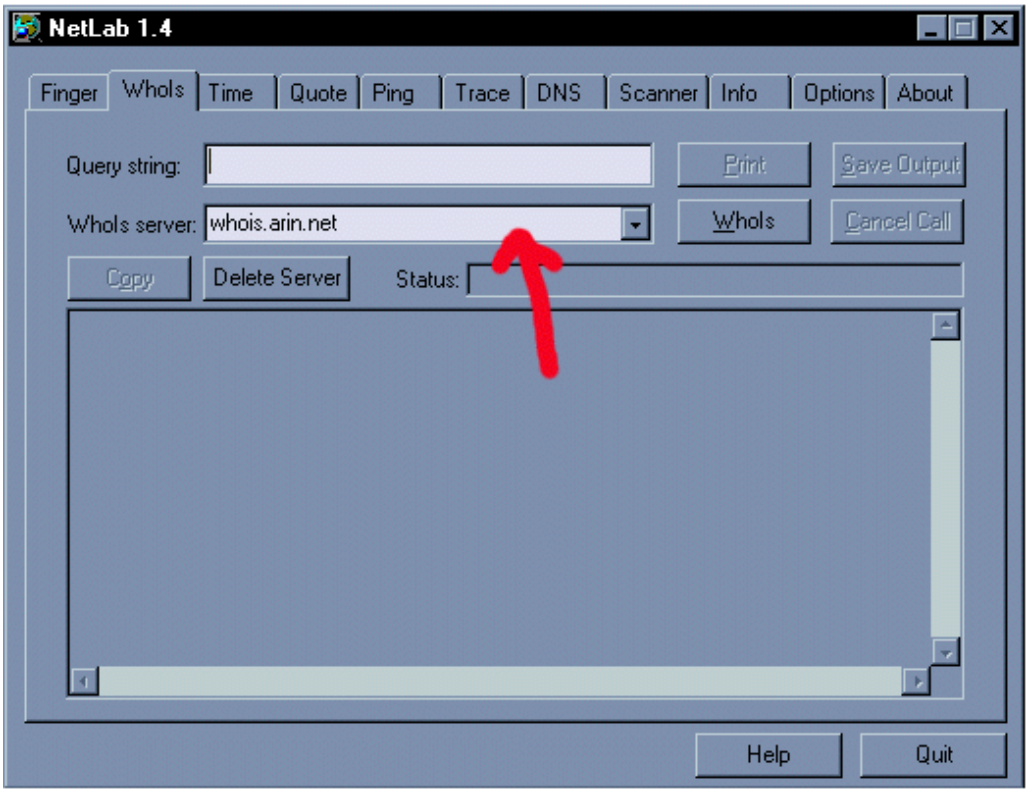
At this point you will see one of two results. You will see a response indicating either the person is online or you will see no response indicating they are offline. We do this to check if the person is still connected.



1: This is the IP address that you are pinging

2: The time it takes to ping the address.

The next step is to check who the IP address belongs to. You can do this by using **whois.arin.net** on the person's IP address.



Once you've typed in the IP address in **Query String** Click on the **Whois** button. You will then see who the IP address belongs to.

This will reveal who the "hackers" internet service provider is. This is very important, if you can figure out where your attacker is coming from you can forward the appropriate information to the right people.

Let's recap our procedure in a step-by-step format.

A) Drop to the DOS prompt

B) Run netstat to check if they got through

C) Start Netlab and do a Ping Test to check if they are still connected

D) Do a Whois (Using the whois.arin.net) lookup

Once you've done the steps above you will need to send the information to your ISP and the attacker's ISP. The goal is to give them as much information as you can about the attacker. Both firewall programs (Black Ice Defender) and (Lockdown 2000) create log files of each attack. Copy the information along with your own test and include the times of each attack into an email and send it to your ISP provider. Send a copy of that email to your attacker's ISP provider also.

(Note: You may need to call the attackers ISP provider in order to get the right Email Address. If the call will involve long distance charges send the message to support@thehackersisp.com)

All ISP providers have an Abuse department. They are responsible for dealing with such issues. If you send the email to the support department of the "hackers" ISP they will forward it to the correct division.

It is your responsibility to report any attacks being made against your computer. I encourage you to take an active part in reporting repeated attacks from the same IP address against your computer, as these are clear indications of someone targeting you.

It may be that you have something they are interested in, or perhaps your system has been compromised prior to your realization, and with the installation of the firewall program you are now blocking their attacks. Whatever the reason now that you are aware your goal is to protect your privacy.

Chapter

10

FINAL WORDS

Congratulations! You've made it to the end of the manual. That's probably not an accomplishment for books of the same length. But this manual is different. You can always make reference back to this manual whenever you have questions. It's like a manual and course in one. Learning the system loop holes and tricks that "hackers" use is only half the process. Protecting your privacy is 90% up to you, the rest can be handled by software.

You have the means and ability to protect yourself. By reading this manual alone you have proven that. You may think to yourself that you're out gunned on the Internet, don't. We all have to start learning from somewhere. Even hackers and so called "hackers" had to start learning somewhere. No one was born with the knowledge of how a computer works.

The Internet is a tool by which many of these "hackers" educate themselves. You can do the same. It remains the most powerful tool for information and development there is.

More and more businesses and services are migrating to the online world. You can either, sit back and watch it go, or jump on the bandwagon and ride it out. It's all up to you.

Exercise caution when dealing with people online, but don't be too paranoid. Enjoy the power of the Internet it can be a great asset to you or your business.

The online population is growing exponentially. With the recent growth of dedicated access your computer is connected to the Internet 24hrs a day. High speed access gives you the opportunity to download files at lightning fast rates. It's a long way from the old dial up BBS's. As technology increases so must your awareness.

Realistically most of us don't care about the inner workings of the Internet. Perhaps we have a sheer curiosity of what happens behind the scenes, but none of us really believes it makes a lot of difference to us to know that information. We primarily care about getting our daily activities done and enjoying the power of the Internet. We want to be able to Log online talk to our friends and family and use the Internet as tool for our benefit.

The Internet connects you to the world where if a friends from Australia wishes to talk to you live one on one they can flip on their webcams turn on their mics and have a video conference. It's a cut above a phone call for a fraction of the price. Don't let "hackers" turn future advancements into unwanted nightmares.

You as a user can prevent this by being careful. Take the extra necessary steps to protect yourself. When compared to the benefits you can have it definitely is worth an extra 1hr-2hrs of your time.

Don't stop learning, read all you can. Why not? You've got the world at your fingertips and information at every turn. But most importantly when all is said and done, take back your privacy from those who may seek to compromise it.

With Great Respect

S&C Enterprises
Consultation Group