

# [Full-Disclosure] ron1n phone home, episode 4

**Source:** <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-04/0302.html>

---

**From:** Bugtraq Security Systems (*research\_at\_bugtraq.org*)

**Date:** 04/07/04

To: full-disclosure@lists.netsys.com

Date: Wed, 7 Apr 2004 09:00:03 -0400

Dear list,

To continue with our Mostly Harmless Hacking series we present you with cutting edge techniques to hack from even the "lamest of on-line services". Today. Enjoy.

With regards,  
Team Bugtraq Security

---

## GUIDE TO (mostly) HARMLESS HACKING

Beginners' Series #2, Section 3.

Hacking from Windows 3.x, 95 and NT

---

This lesson will tell you how, armed with even the lamest of on-line services such as America Online and the Windows 95 operating system, you can do some fairly serious Internet hacking -- today!

In this lesson we will learn how to:

- Use secret Windows 95 DOS commands to track down and port surf computers used by famous on-line service providers.
- Telnet to computers that will let you use the invaluable hacker tools of whois, nslookup, and dig.
- Download hacker tools such as port scanners and password crackers designed for use with Windows.
- Use Internet Explorer to evade restrictions on what programs you can run on your school or work computers.

Yes, I can hear jericho and Rogue Agent and all the other Super Duper hackers on this list laughing. I'll bet already they have quit reading this and are furiously emailing me flames and making phun of me in 2600 meetings. Windows hacking? Pooh!

Tell seasoned hackers that you use Windows and they will laugh at you. They'll tell you to go away and don't come back until you're armed with a shell account or some sort of Unix on your PC. Actually, I have long shared their opinion. Shoot, most of the time hacking from Windoze is like using a 1969 Volkswagon to race against a dragster using one of VP Racing's high-tech fuels.

But there actually is a good reason to learn to hack from Windows. Some of your best tools for probing and manipulating Windows networks are found only on Windows NT. Furthermore, with Win 95 you can practice the Registry hacking that is central to working your will on Win NT servers and the networks they administer.

In fact, if you want to become a serious hacker, you eventually will have to learn Windows. This is because Windows NT is fast taking over the Internet from Unix. An IDC report projects that the Unix-based Web server market share will fall from the 65% of 1995 to only 25% by the year 2000. The Windows NT share is projected to grow to 32%. This weak future for Unix Web servers is reinforced by an IDC report reporting that market share of all Unix systems is now falling at a compound annual rate of decline of -17% for the foreseeable future, while Windows NT is growing in market share by 20% per year. (Mark Winther, "The Global Market for Public and Private Internet Server Software," IDC #11202, April 1996, 10, 11.)

So if you want to keep up your hacking skills, you're going to have to get wise to Windows. One of these days we're going to be sniggering at all those Unix-only hackers.

Besides, even poor, pitiful Windows 95 now can take advantage of lots of free hacker tools that give it much of the power of Unix.

Since this is a beginners' lesson, we'll go straight to the Big Question: "All I got is AOL and a Win 95 box. Can I still learn how to hack?"

Yes, yes, yes!

The secret to hacking from AOL/Win 95 — or from any on-line service that gives you access to the World Wide Web — is hidden in Win 95's MS-DOS (DOS 7.0).

DOS 7.0 offers several Internet tools, none of which are documented in either the standard Windows or DOS help features. But you're getting the chance to learn these hidden features today.

So to get going with today's lesson, use AOL or whatever lame on-line service you may have and make the kind of connection you use to get on the

Web (this will be a PPP or SLIP connection). Then minimize your Web browser and prepare to hack! Next, bring up your DOS window by clicking Start, then Programs, then MS-DOS.

For best hacking I've found it easier to use DOS in a window with a task bar which allows me to cut and paste commands and easily switch between Windows and DOS programs. If your DOS comes up as a full screen, hold down the Alt key while hitting enter, and it will go into a window. Then if you are missing the task bar, click the system menu on the left side of the DOS window caption and select Toolbar.

Now you have the option of eight TCP/IP utilities to play with: telnet, arp, ftp, nbtstat, netstat, ping, route, and tracert.

Telnet is the biggie. You can also access the telnet program directly from Windows. But while hacking you may need the other utilities that can only be used from DOS, so I like to call telnet from DOS.

With the DOS telnet you can actually port surf almost as well as from a Unix telnet program. But there are several tricks you need to learn in order to make this work.

First, we'll try out logging on to a strange computer somewhere. This is a fun thing to show your friends who don't have a clue because it can scare the heck out of them. Honest, I just tried this out on a neighbor. He got so worried that when he got home he called my husband and begged him to keep me from hacking his work computer!

To do this (I mean log on to a strange computer, not scare your neighbors) go to the DOS prompt C:\WINDOWS> and give the command "telnet." This brings up a telnet screen. Click on Connect, then click Remote System.

This brings up a box that asks you for "Host Name." Type "whois.internic.net" into this box. Below that it asks for "Port" and has the default value of "telnet." Leave in "telnet" for the port selection. Below that is a box for "TermType." I recommend picking VT100 because, well, just because I like it best.

The first thing you can do to frighten your neighbors and impress your friends is a "whois." Click on Connect and you will soon get a prompt that looks like this:

```
[vt100]InterNIC>
```

Then ask your friend or neighbor his or her email address. Then at this InterNIC prompt, type in the last two parts of your friend's email address. For example, if the address is "luser@aol.com," type in "aol.com."

Now I'm picking AOL for this lesson because it is really hard to hack. Almost any other on-line service will be easier.

For AOL we get the answer:

```
[vt100] InterNIC > whois aol.com
```

```
Connecting to the rs Database . . . . .
```

```
Connected to the rs Database
```

```
America Online (AOL-DOM)
```

```
12100 Sunrise Valley Drive
```

```
Reston, Virginia 22091
```

```
USA
```

```
Domain Name: AOL.COM
```

```
Administrative Contact:
```

```
O'Donnell, David B (DBO3) PMDAtropos@AOL.COM
```

```
703/453-4255 (FAX) 703/453-4102
```

```
Technical Contact, Zone Contact:
```

```
America Online (AOL-NOC) trouble@aol.net
```

```
703-453-5862
```

```
Billing Contact:
```

```
Barrett, Joe (JB4302) BarrettJG@AOL.COM
```

```
703-453-4160 (FAX) 703-453-4001
```

```
Record last updated on 13-Mar-97.
```

```
Record created on 22-Jun-95.
```

```
Domain servers in listed order:
```

```
DNS-01.AOL.COM 152.163.199.42
```

```
DNS-02.AOL.COM 152.163.199.56
```

```
DNS-AOL.ANS.NET 198.83.210.28
```

These last three lines give the names of some computers that work for America Online (AOL). If we want to hack AOL, these are a good place to start.

```
*****
```

Newbie note: We just got info on three "domain name servers" for AOL. "Aol.com" is the domain name for AOL, and the domain servers are the computers that hold information that tells the rest of the Internet how to send messages to AOL computers and email addresses.

```
*****
```

```
*****
```

Evil genius tip: Using your Win 95 and an Internet connection, you can run a whois query from many other computers, as well. Telnet to your target computer's port 43 and if it lets you get on it, give your query.

Example: telnet to nic.ddn.mil, port 43. Once connected type "whois DNS-01.AOL.COM," or whatever name you want to check out. However, this only works on computers that are running the whois service on port 43.

Warning: show this trick to your neighbors and they will really be terrified. They just saw you accessing a US military computer! But it's OK, nic.ddn.mil is open to the public on many of its ports. Check out its Web site [www.nic.ddn.mil](http://www.nic.ddn.mil) and its ftp site, too --- they are a mother lode of

information that is good for hacking.

\*\*\*\*\*

Next I tried a little port surfing on DNS-01.AOL.COM but couldn't find any ports open. So it's a safe bet this computer is behind the AOL firewall.

\*\*\*\*\*

Newbie note: port surfing means to attempt to access a computer through several different ports. A port is any way you get information into or out of a computer. For example, port 23 is the one you usually use to log into a shell account. Port 25 is used to send email. Port 80 is for the Web. There are thousands of designated ports, but any particular computer may be running only three or four ports. On your home computer your ports include the monitor, keyboard, and modem.

\*\*\*\*\*

So what do we do next? We close the telnet program and go back to the DOS window. At the DOS prompt we give the command "tracert 152.163.199.42." Or we could give the command "tracert DNS-01.AOL.COM." Either way we'll get the same result. This command will trace the route that a message takes, hopping from one computer to another, as it travels from my computer to this AOL domain server computer. Here's what we get:

```
C:\WINDOWS>tracert 152.163.199.42
```

```
Tracing route to dns-01.aol.com [152.163.199.42]
over a maximum of 30 hops:
```

```
 1 * * * Request timed out.
 2 150 ms 144 ms 138 ms 204.134.78.201
 3 375 ms 299 ms 196 ms glory-cyberport.nm.westnet.net [204.134.78.33]
 4 271 ms * 201 ms enss365.nm.org [129.121.1.3]
 5 229 ms 216 ms 213 ms h4-0.cnss116.Albuquerque.t3.ans.net
 [192.103.74.45]
 6 223 ms 236 ms 229 ms f2.t112-0.Albuquerque.t3.ans.net
 [140.222.112.221]
 7 248 ms 269 ms 257 ms h14.t64-0.Houston.t3.ans.net [140.223.65.9]
 8 178 ms 212 ms 196 ms h14.t80-1.St-Louis.t3.ans.net [140.223.65.14]
 9 316 ms * 298 ms h12.t60-0.Reston.t3.ans.net [140.223.61.9]
10 315 ms 333 ms 331 ms 207.25.134.189
11 * * * Request timed out.
12 * * * Request timed out.
13 207.25.134.189 reports: Destination net unreachable.
```

What the heck is all this stuff? The number to the left is the number of computers the route has been traced through. The "150 ms" stuff is how long, in thousandths of a second, it takes to send a message to and from that computer. Since a message can take a different length of time every time you send it, tracert times the trip three times. The "\*" means the trip was taking too long so tracert said "forget it." After the timing info comes the name of the computer the message reached, first in a form that is easy for a

human to remember, then in a form — numbers — that a computer prefers.

“Destination net unreachable” probably means tracer hit a firewall.

Let’s try the second AOL domain server.

```
C:\WINDOWS>tracert 152.163.199.56
```

```
Tracing route to dns-02.aol.com [152.163.199.56]  
over a maximum of 30 hops:
```

```
 1 * * * Request timed out.  
 2 142 ms 140 ms 137 ms 204.134.78.201  
 3 246 ms 194 ms 241 ms glory-cyberport.nm.westnet.net [204.134.78.33]  
 4 154 ms 185 ms 247 ms enss365.nm.org [129.121.1.3]  
 5 475 ms 278 ms 325 ms h4-0.cnss116.Albuquerque.t3.ans.net [192.103.74.  
45]  
 6 181 ms 187 ms 290 ms f2.t112-0.Albuquerque.t3.ans.net [140.222.112.22  
1]  
 7 162 ms 217 ms 199 ms h14.t64-0.Houston.t3.ans.net [140.223.65.9]  
 8 210 ms 212 ms 248 ms h14.t80-1.St-Louis.t3.ans.net [140.223.65.14]  
 9 207 ms * 208 ms h12.t60-0.Reston.t3.ans.net [140.223.61.9]  
10 338 ms 518 ms 381 ms 207.25.134.189  
11 * * * Request timed out.  
12 * * * Request timed out.  
13 207.25.134.189 reports: Destination net unreachable.
```

Note that both tracerts ended at the same computer named h12.t60-0.Reston.t3.ans.net. Since AOL is headquartered in Reston, Virginia, it’s a good bet this is a computer that directly feeds stuff into AOL. But we notice that h12.t60-0.Reston.t3.ans.net , h14.t80-1.St-Louis.t3.ans.net, h14.t64-0.Houston.t3.ans.net and Albuquerque.t3.ans.net all have numerical names beginning with 140, and names that end with “ans.net.” So it’s a good guess that they all belong to the same company. Also, that “t3” in each name suggests these computers are routers on a T3 communications backbone for the Internet.

Next let’s check out that final AOL domain server:

```
C:\WINDOWS>tracert 198.83.210.28
```

```
Tracing route to dns-aol.ans.net [198.83.210.28]  
over a maximum of 30 hops:
```

```
 1 * * * Request timed out.  
 2 138 ms 145 ms 135 ms 204.134.78.201  
 3 212 ms 191 ms 181 ms glory-cyberport.nm.westnet.net [204.134.78.33]  
 4 166 ms 228 ms 189 ms enss365.nm.org [129.121.1.3]  
 5 148 ms 138 ms 177 ms h4-0.cnss116.Albuquerque.t3.ans.net [192.103.74.  
45]  
 6 284 ms 296 ms 178 ms f2.t112-0.Albuquerque.t3.ans.net [140.222.112.22
```

1]

7 298 ms 279 ms 277 ms h14.t64-0.Houston.t3.ans.net [140.223.65.9]  
8 238 ms 234 ms 263 ms h14.t104-0.Atlanta.t3.ans.net [140.223.65.18]  
9 301 ms 257 ms 250 ms dns-aol.ans.net [198.83.210.28]

Trace complete.

Hey, we finally got all the way through to something we can be pretty certain is an AOL box, and it looks like it's outside the firewall! But look at how the tracer took a different path this time, going through Atlanta instead of St. Louis and Reston. But we are still looking at ans.net addresses with T3s, so this last nameserver is using the same network as the others.

Now what can we do next to get luser@aol.com really wondering if you could actually break into his account? We're going to do some port surfing on this last AOL domain name server! But to do this we need to change our telnet settings a bit.

Click on Terminal, then Preferences. In the preferences box you need to check "Local echo." You must do this, or else you won't be able to see everything that you get while port surfing. For some reason, some of the messages a remote computer sends to you won't show up on your Win 95 telnet screen unless you choose the local echo option. However, be warned, in some situations everything you type in will be doubled. For example, if you type in "hello" the telnet screen may show you "heh lelllo o. This doesn't mean you mistyped, it just means your typing is getting echoed back at various intervals.

Now click on Connect, then Remote System. Then enter the name of that last AOL domain server, dns-aol.ans.net. Below it, for Port choose Daytime. It will send back to you the day of the week, date and time of day in its time zone.

Aha! We now know that dns-aol.ans.net is exposed to the world, with at least one open port, heh, heh. It is definitely a prospect for further port surfing. And now your friend is wondering, how did you get something out of that computer?

\*\*\*\*\*

Clueless newbie alert: If everyone who reads this telnets to the daytime port of this computer, the sysadmin will say "Whoa, I'm under heavy attack by hackers!!! There must be some evil exploit for the daytime service! I'm going to close this port pronto!" Then you'll all email me complaining the hack doesn't work. Please, try this hack out on different computers and don't all beat up on AOL.

\*\*\*\*\*

Now let's check out that Reston computer. I select Remote Host again and enter the name h12.t60-0.Reston.t3.ans.net. I try some port surfing without success. This is a seriously locked down box! What do we do next?

So first we remove that “local echo” feature, then we telnet back to whois.internic. We ask about this ans.net outfit that offers links to AOL:

```
[vt100] InterNIC > whois ans.net
```

```
Connecting to the rs Database . . . . .  
Connected to the rs Database  
ANS CO+RE Systems, Inc. (ANS-DOM)  
100 Clearbrook Road  
Elmsford, NY 10523
```

```
Domain Name: ANS.NET
```

```
Administrative Contact:
```

```
Hershman, Ittai (IH4) ittai@ANS.NET  
(914) 789-5337
```

```
Technical Contact:
```

```
ANS Network Operations Center (ANS-NOC) noc@ans.net  
1-800-456-6300
```

```
Zone Contact:
```

```
ANS Hostmaster (AH-ORG) hostmaster@ANS.NET  
(800)456-6300 fax: (914)789-5310
```

```
Record last updated on 03-Jan-97.
```

```
Record created on 27-Sep-90.
```

```
Domain servers in listed order:
```

```
NS.ANS.NET 192.103.63.100  
NIS.ANS.NET 147.225.1.2
```

Now if you wanted to be a really evil hacker you could call that 800 number and try to social engineer a password out of somebody who works for this network. But that wouldn't be nice and there is nothing legal you can do with ans.net passwords. So I'm not telling you how to social engineer those passwords.

Anyhow, you get the idea of how you can hack around gathering info that leads to the computer that handles anyone's email.

So what else can you do with your on-line connection and Win 95?

Well... should I tell you about killer ping? It's a good way to lose your job and end up in jail. You do it from your Windows DOS prompt. Find the gory details in the GTMHH Vol.2 Number 3, which is kept in one of our archives listed at the end of this lesson. Fortunately most systems administrators have patched things nowadays so that killer ping won't work. But just in case your ISP or LAN at work or school isn't protected, don't test it without your sysadmin's approval!

Then there's ordinary ping, also done from DOS. It's sort of like traceroute, but all it does is time how long a message takes from one computer to another, without telling you anything about the computers between yours and the one you ping.

Other TCP/IP commands hidden in DOS include:

- Arp IP-to-physical address translation tables
- Ftp File transfer protocol. This one is really lame. Don't use it. Get a shareware Ftp program from one of the download sites listed below.
- Nbtstat Displays current network info --- super to use on your own ISP
- Netstat Similar to Nbtstat
- Route Controls router tables --- router hacking is considered extra elite.

Since these are semi-secret commands, you can't get any details on how to use them from the DOS help menu. But there are help files hidden away for these commands.

- For arp, nbtstat, ping and route, to get help just type in the command and hit enter.
- For netstat you have to give the command "netstat ?" to get help.
- Telnet has a help option on the tool bar.

I haven't been able to figure out a trick to get help for the ftp command.

Now suppose you are at the point where you want to do serious hacking that requires commands other than these we just covered, but you don't want to use Unix. Shame on you! But, heck, even though I usually have one or two Unix shell accounts plus Walnut Creek Slackware on my home computer, I still like to hack from Windows. This is because I'm ornery. So you can be ornery, too.

So what is your next option for doing serious hacking from Windows?

How would you like to crack Win NT server passwords? Download the free Win 95 program NTLocksmith, an add-on program to NTRecover that allows for the changing of passwords on systems where the administrative password has been lost. It is reputed to work 100% of the time. Get both NTLocksmith and NTRecover --- and lots more free hacker tools --- from <http://www.ntinternals.com>.

\*\*\*\*\*

You can go to jail warning: If you use NTRecover to break into someone else's system, you are just asking to get busted.

\*\*\*\*\*

How would you like to trick your friends into thinking their NT box has crashed when it really hasn't? This prank program can be downloaded from <http://www.osr.com/insider/insdrcod.htm>.

\*\*\*\*\*

You can get punched in the nose warning: need I say more?

\*\*\*\*\*

But by far the deadliest hacking tool that runs on Windows can be downloaded from, guess what?

<http://home.microsoft.com>

That deadly program is Internet Explorer 3.0. Unfortunately, this program is even better for letting other hackers break into your home computer and do stuff like make your home banking program (e.g. Quicken) transfer your life savings to someone in Afghanistan.

But if you're aren't brave enough to run Internet Explorer to surf the Web, you can still use it to hack your own computer, or other computers on your LAN. You see, Internet Explorer is really an alternate Windows shell which operates much like the Program Manager and Windows Explorer that come with the Win 94 and Win NT operating systems.

Yes, from Internet Explorer you can run any program on your own computer. Or any program to which you have access on your LAN.

\*\*\*\*\*

Newbie note: A shell is a program that mediates between you and the operating system. The big deal about Internet Explorer being a Windows shell is that Microsoft never told anyone that it was in fact a shell. The security problems that are plaguing Internet Explorer are mostly a consequence of it turning out to be a shell. By contrast, the Netscape and Mosaic Web browsers are not shells. They also are much safer to use.

\*\*\*\*\*

To use Internet Explorer as a Windows shell, bring it up just like you would if you were going to surf the Web. Kill the program's attempt to establish an Internet connection — we don't want to do anything crazy, do we?

Then in the space where you would normally type in the URL you want to surf, instead type in c:.

Whoa, look at all those file folders that come up on the screen. Look familiar? It's the same stuff your Windows Explorer would show you. Now for fun, click "Program Files" then click "Accessories" then click "MSPaint." All of a sudden MSPaint is running. Now paint your friends who are watching this hack very surprised.

Next close all that stuff and get back to Internet Explorer. Click on the Windows folder, then click on Regedit.exe to start it up. Export the password file (it's in HKEY\_CLASSES\_ROOT). Open it in Word Pad. Remember, the ability to control the Registry of a server is the key to controlling the network it serves. Show this to your next door neighbor and tell her that you're going to use Internet Explorer to surf her password files. In a few hours the Secret Service will be fighting with the FBI on your front lawn over who gets to try to bust you. OK, only kidding here.

So how can you use Internet Explorer as a hacking tool? One way is if you are using a computer that restricts your ability to run other programs on your computer or LAN. Next time you get frustrated at your school or library computer, check to see if it offers Internet Explorer. If it does, run it and try entering disk drive names. While C: is a common drive on your home computer, on a LAN you might get results by putting in R: or Z: or any other letter of the alphabet.

Next cool hack: try automated port surfing from Windows! Since there are thousands of possible ports that may be open on any computer, it could take days to fully explore even just one computer by hand. A good answer to this problem is the NetCop automated port surfer, which can be found at <http://www.netcop.com/>.

Now suppose you want to be able to access the NTFS file system that Windows NT uses from a Win 95 or even DOS platform? This can be useful if you are wanting to use Win 95 as a platform to hack an NT system. <http://www.ntinternals.com/ntfsdos.htm> offers a program that allows Win 95 and DOS to recognize and mount NTFS drives for transparent access.

Hey, we are hardly beginning to explore all the wonderful Windows hacking tools out there. It would take megabytes to write even one sentence about each and every one of them. But you're a hacker, so you'll enjoy exploring dozens more of these nifty programs yourself. Following is a list of sites where you can download lots of free and more or less harmless programs that will help you in your hacker career:

<ftp://ftp.cdrom.com>  
<ftp://ftp.coast.net>  
<http://hertz.njit.edu/%7ebxg3442/temp.html>  
<http://www.alpworld.com/infinity/void-neo.html>  
<http://www.danworld.com/nettools.html>  
<http://www.eskimo.com/~nwps/index.html>  
<http://www.geocities.com/siliconvalley/park/2613/links.html>  
<http://www.ilf.net/Toast/>  
<http://www.islandnet.com/~cliffmcc>  
<http://www.simtel.net/simtel.net>  
<http://www.supernet.net/cwsapps/cwsa.html>  
<http://www.trytel.com/hack/>  
<http://www.tucows.com>  
<http://www.windows95.com/apps/>  
<http://www2.southwind.net/%7emiker/hack.html>

---

Want to see back issues of Guide to (mostly) Harmless Hacking? See either <http://www.tacd.com/zines/gtmhh/> or <http://ra.nilenet.com/~mjl/hacks/codez.htm> or <http://www3.ns.sympatico.ca/loukas.halo8/HappyHacker/>  
Subscribe to our email list by emailing to [hacker@techbroker.com](mailto:hacker@techbroker.com) with message "subscribe" or join our Hacker forum at <http://www.infowar.com/cgi-shl/login.exe>.

Full-Disclosure: [Full-Disclosure] ron1n phone home, episode 4

Chat with us on the Happy Hacker IRC channel. If your browser can use Java, just direct your browser to [www.infowar.com](http://www.infowar.com), click on chat, and choose the #hackers channel.

Want to share some kewl stufh with the Happy Hacker list? Correct mistakes? Send your messages to [hacker@techbroker.com](mailto:hacker@techbroker.com). To send me confidential email (please, no discussions of illegal activities) use [cmein@techbroker.com](mailto:cmein@techbroker.com) and be sure to state in your message that you want me to keep this confidential. If you wish your message posted anonymously, please say so! Direct flames to [dev/null@techbroker.com](mailto:dev/null@techbroker.com). Happy hacking!  
Copyright 1997 Carolyn P. Meinel. You may forward or post this GUIDE TO (mostly) HARMLESS HACKING on your Web site as long as you leave this notice at the end.

---

Carolyn Meinel  
M/B Research -- The Technology Brokers

---

Full-Disclosure - We believe in it.  
Charter: <http://lists.netsys.com/full-disclosure-charter.html>