written Today [04-APR-98]

Back again ;p It's been a while since the last one...I'll talk more about the my where abouts at the end of this one. I am glad to be back, and I like coming back to some fairly uncharted territory for the Mac Underground.

I recently mad the acquaintance of a couple of up-and-comers who are keepin' the cause alive. Freaky, #su98(EfNet) runs an ambitious take over crew. One of his peers The Weasel runs a very nice Hotline MacHack site that can be found with your Hotline client at hackadict.ml.org. A regular on The Weasels page, and object of attention for this piece is a Mac UG programmer named Weedo.

WeeDo is avid fan of the Mac underground, and a coder of considerable potential, he's succeffuly expored some ways in which the Mac UG can spoof via TCP/IP clients.... something which to my knowledge hasn't been accomlished yet.

Sure we can spoof via a connection to a Linux box and runnin JIZ, but thats a little different. WeeDo came up with a script that when utilized in conjunction with an exploit of a software facility called WinGate (more on that in next section) will allow you to spoof right through IRCle... Not to bad...so thats the topic of todays lessson...

inGate is a software product of a New Zealand company called Firefly, Ltd. What the program essentially is, is a Firewall/Proxy server for the masses. It's a cheap, fairly well

written internet gateway... You run the thing on any PC running Windows 95 or NT, and it makes a connection to the internet, and every computer connected to that machine via the LAN, can connect to the internet through that machine. Where in lies the popularity of it... i.e. A small business with a LAN of 3 or 4 computers, can now go out and get a cheap 486 or Pentium, fortify it with some memory a fast modem and a 10/baseT card, get a dedicated Internet account, and then hook up the rest of the computers on the LAN to that one and they can all have dedicated Internet access.

ne modem, one phone line, one internet account, but access for as many as their are on the LAN. Hell of a money saver. On the Mac side we have a similar program called Vicom Internet Gateway. Some of you may have heard of it.

Ok...now here's the thing so we have this program called WinGate, and it's this firewall/proxy server. So what? How does it let us spoof.. Well besides being this proxy server it has some other would be nice features which include:

(from the promo sheet)

* SOCKS V5 Server
* WWW Proxy
* HTTP Caching
* Request Types
* Accounting
* Auditing / Logging
* Policies and Rights
* FTP Gateway
* Telnet Gateway
* VDOLive Proxy
* POP3 Proxy
* Real Audio Proxy
* Mapped Links

* Rules
* Dial On Demand

A nice set of features...especially given this thing of downloadable off the net with a free trial... A pretty nice package.

you may have noticed in bold a Telnet gateway. Firefly's description of this feature is:

> The Telnet Gateway allows use of Telnet clients to connect to remote servers.

DOH! There in lies our spoof. And not because of this feature in and of itself...but because od a bundling mistake.

Essentially what we are talking about here is not really spoofing, no more so than if you dial in to a legitimate shell account that you own, and from that shell account type: `telnet`, and telnet from shell account to another site. I guess in some definitions thats spoofing, but I don't know...it seems pretty par for the course as far as UNIX shells go. I mean you've always been able to do that.

Well the problem with WinGate is that the programmers didn't see any immediate reason to set the telnet gateway up with a password. lol So essentially, you don't need to be a 'legitimate' user to use the telnet function of a remote server. Or, more appropriatley stated, since no password is necessary by default, _EVERYONE_ is a legitimate user! lol So in other words, you have but to find a WinGate, and if it has no telnet gateway password set, then feel free to telnet back out of it, in which case all further connection will appear (and accurately so) to be originating from the WinGate you telnetted into.

And the icing on the cake is, not only does this thing not require a password to use the telnet gateway by default, by default it also doesn't log incoming connections. In fact, the low end version of this package doesn't even offer logging. So though we're not talking about true spoofing here, (imho), we are talking about 'sploit' heaven >snicker<

ell great, now we know (sort of) what we can do with WinGates, what the hell good is it if we don't know how to find them. Well I told you of the sweetness of the cake, I told you of the icing on the cake, now here's the cherry on top: WinGates ain't hard to find ;)

As I have said, you can download this thing off the net, and it's a very popular program, so alot of people are using WinGates, and it just so happens Firefly chose to include a TCP listening port (for what reason I have no clue), but that port is at 1080, and with the right tool, you can scan for WinGates all day.

Right tool? If you don't have it...get it NOW! AGNetTools from the AGGroup, the nicest suite of Internet network tools to be released for the Mac in a LONG time. It's free, and more over, YOU NEED IT to find WinGates. Here's the URL....

ftp://ftp.aggroup.com/Public/goodies/AGNetTools/

Ok, once you've picked up NetTools...load it, and lets get busy.... We need to scan for IPs hosting WinGates. To find them we will use the NetTools Service Scan and search for machines listening at port 1080.

Iright, we select a Service Scan, and it brings up the Service Scan window. We need to do 2 things to proceed with the scan, first we need to make sure that the port we're searching for is set at 1080 (VITAL), and second we need to select a range to scan for.

For this example we're just going to scan a single Class C. from:

207.0.167.0 to
207.0.167.255

This will scan 255 IPs. Normally you won't be so lucky as to find a WinGate in searching a single Class C. We will for this piece ;) but thats only because I already did my homework. The scan I would suggest if you wanna scan in an evening is :

xxx.xx0.xxx.xxx to
xxx.xx1.xxx.xxx

This will scan out (I believe) 65,025 address, or 255 x 255. Not sure at how I came to that conclusion, but anyway, I recommend that scan pattern only because I know that if you try and do more than that AGNetTools will crash. I think the nimbers get too high for it or somethin. Whatever the case, if you try and do more, or try to scan something like 000.000.000.000 to 255.255.255.255, it shuts down your machine.

So...chill...I guarantee you if you scan 65,025 addresses you will find PLENTY of WinGates.

Anyway for our example we only scanned 255...and this is what the scan looks like:

Iright, We performed a scan of an entire Class C from 207.0.167.0 to 207.76.0.255. At port 1080, the Service Scan found a number of ports, open, but as you recall, we're not interested in UDP ports, only TCP ports. And of those there is only one. 207.0.167.206 or www.casi400.com. But one is all we need, so good enough. At this point we can bring on IRCIe and WeeDo's script that we mentioned early on...

lright, we have WinGates, now we can begin doing some (pseudo-) spoofing. I say (pseudo-) because more acturally what we are doing is telnet redirection. We're telnetting into insecure WinGates, and using their built-in telnet servers to telnet back out from those WinGates thus leaving our originating source to appear to be coming from that WinGate. And because the IRC is essentially nothing more than a slightly modified telnet connection we can use WinGates to 'spoof' on the IRC, making it appear as though our address is something other than our address... which technically it is =p Anyway...

To help us exploit these WinGates holes, and utilize them to spoof our addy on the IRC, we have a helpful little IRCle script from the Up-And-Comer I mentioned earlier, WeeDo.

Here's WeeDo's script as follows...

break down of what the script does...

1.
First, when the script is loaded, it displays USAGE instructions

2.
Next, as normal you connect to a server with the /SERVER command, with

the exception that instead of connecting to an IRC server, you connect to

one of the
WinGates we found earlier. (i.e. 207.0.167.0)

3.
Once we've Connected to a WinGate, we use the script's '/SPOOF'

command. As you can see, essentially what the '/SPOOF' command does is

send the server our
defined NICK
IRCSERVER IRCSERVERPORT IDENT

and TAGLINE, via the IRCD

/QUOTE command.

We use the script to do it for us, because although we could use the /quote command directly to send the IRC parameters through, we probably couldn't type then fast enough to make the connection. We'd more than likely get an...

*** USER Not enough parameters

...error. So to that extent of utility, the script is right on time for what it does.

Ok so now we know the mechanics of the script, time to bring on IRCle, and use our script to start 'spoofing'.

f you don't have it, stop by and get the latest version of IRCle.

http://www.xs4all.nl/~ircle

This hack only works (as far as I know) with version b10 or better. Once you've got IRCle at hand, make sure that the WeeDo's spoofer is in IRCle's script folder. Once Ircle is loaded, we can get to spoofin'...

bove is a picture of IRCle's four main panels, The Console, the Userlist, the Connections, and the input line. For sake of ease of reading we'll show the windows seperatley from this time forth as needed, with the exception of the console which we will show dumped to directly to the screen as a text dump.

Alright, the first thing we need to do in IRCle is load the spoofer...

console:)

Spoofer 1.2 loaded...

Usage:

1. '/server [wingate ip] [telnetport]'
2. Wait until connection...
3. '/spoof [nick] [ircserver] [ircserverport] [ident] [tagline]'

A wonderful spoof from WeeDo, original code by Photoman

Ok...now that WeeDo's spoofer is loaded we need to go ahead and try and make a connection to the WinGate we found in AGNetTools...

You may have recall that we found the WinGate at 207.0.167.206 at port 1080. Well with out going into much detail, the main thing to keep in mind is that 1080 is just a real useful port for searching for WinGates. But to use thae WinGate to spoof any given protocol we have to use the port assigned for that protocol. In the case of IRC, the port is 23.... 23 being the standard port for Telnet, and IRC essentially being nothing more than a worked over telnet connection. So we will attempt to connect to IP we found but at port 23...

ooking up IP number for 207.0.167.206:23
Found IP number: 207.0.167.206
Identd waiting for connection
Contacting server 207.0.167.206:23
Connection with 207.0.167.206:23 established
unknown server message!: ÿûÿûÿ‡WinGate>NICK oB
unknown server message!: Connecting to host NICK...Host name lookup for 'NICK' failed
unknown server message!: USER oleBuzzard 32 . :/<n0wledge phreak
unknown server message!: Connecting to host USER oleBuzzard 32 . ...Host name lookup for 'USER oleBuzzard 32 . ' failed

Ok, see all that crap up there in red...well that's what the telnet connection to the WinGate ends up looking like when it comes back from the WinGate server, through to IRCLe...

Now this is the point where alot of people can get hung up, because once you've gotten this far, it seems like IRCle is just hanging. And to further that assumption, IRCle's connection screen shows the connection as not being all the way open...

ell don't worry about it...this is normal...in effect the connection is not all the way open...mainly because we're connected to the WinGate telnet server, but not yet to the IRC...for that we need to enter the second command line for the spoofer. You might recall it read something like this...:

/spoof [nick] [ircserver] [ircserverport] [ident] [tagline]

Well that's exactly what we're going to do...

nknown server message!: irc.mindspring.com 6667
unknown server message!: Connecting to host irc.mindspring.com...Connected
Looking up your hostname...
Checking Ident
No Ident response
Found your hostname
*** Welcome to the Internet Relay Network oB
*** Your host is irc.mindspring.com, running version 2.8/hybrid-5.1b8
*** Your host is irc.mindspring.com, running version 2.8/hybrid-5.1b8
*** This server was created Wed Nov 26 1997 at 17:30:46 EST
*** 2.8/hybrid-5.1b8 oiwszcrkfydn biklmnopstv
*** There are 5731 users and 28357 invisible on 61 servers
*** There are 207 IRC Operators online
*** 14886 channels have been formed.
*** I have 970 clients and 1 servers
*** Current local users: 970 Max: 1638
*** Current global users: 34088 Max: 42426
*** - irc.mindspring.com Message of the Day -
*** - 3/4/1998 14:21
*** -=-=-=-=-==-
*** MindSpring Enterprises -=- EFNet Internet Relay Chat Server
*** Located in Atlanta, Georgia -=- Operating on Ports 6660-6669
*** --
*** Server Administrator: johanMS
*** Server Ops: Celestian Osc zeppelin Saralee tersIan brian-x
*** Geezus Angmar Bogman
*** -=-
***
*** MindSpring is a full service nationwide Internet Service
*** Provider located in Atlanta, Georgia.
***
*** Please send reports of abusive users of this server to
*** ircadmin@mindspring.com, including logs of the event(s) and
*** the output of the /TIME or /DATE command, as well as
*** /WHOIS.
***
*** This server is a privately owned service and has an Acceptable
*** Use Policy that clients must adhere to. Failure to follow these
*** rules will result in denial of use of the service (K-Line).
***

```
***      * No BOTS. This includes bots used to maintain channels as well
***        as bots used to harass other users.
***
***      * No MULTIPLE CONNECTIONS. One connection is allowed per user.
***
***      * No LINK LOOKERS or automated scripts designed for HACKING.
***
***      * CHANNEL TAKEOVERS, FLOODING, and other forms of IRC ABUSE are
***        absolutely forbidden here.
***
***      * If you start a channel, it is yours to administer. We CAN NOT
***        assist you in the maintenance or recovery of your channel.
***        This is not political but rather technical. There is NO means
***        for an Server Operator to modify the state of ANY channel.
***
***      * No ADVERTISING of any kind.
***
***    We are currently NOT looking for any new IRC Operators
***
*** End of /MOTD command.

*** Notify List:   daemon9 videov free_ TheShark DreamRock Gersh Shells SoMeOnE In- panasync habit
```

Well what'dya know...we did it ;p. Don't believe me? Well check for yourself...do a /whois...

```
** oB is ~oleBuzzard@www.casi400.com (nu-r00lz!)
*** oB is on IRC via server irc.mindspring.com (MindSpring IRC Server)
*** oB has been idle for 1 minutes and 29 seconds
```

You might recall that www.casi400.com was the address where AGNetTools found the WinGate.

ow then, in other fun, what is really nice about this spoof is that you can run up to 10 clones per IRCle IRC client, and have them all come back with different IPs. Now thats

great for getting around bans, and k-lines and such, and also for performing Clone Floods. As some of you may know, if you use something like ACID to flood with under clones, the flood can in effect flood you right off the IRC...well with the multiple addresses, that doesn't have nearly the likelihood of happening....

To Run the clones, just follow the procedures listed throughout this phile, but do it on another of IRCles connection slots. There are ten available.

ere's a list of found WinGates. All of these were scanned with AGNetTools, and verified through IRCle to work for spoofing. Incidentally, these were all found in a single afternoon.

IP Address	Domain Name	Protocol
205.151.63.192	63-192.tr.cgocable.ca	TCP
205.151.63.215	63-215.tr.cgocable.ca	TCP
207.0.21.51	fire.maryville.com	TCP
207.0.21.65	fire2.maryville.com	TCP
207.0.23.10	ns.consolidated.com	TCP
207.0.72.62	xxx-yyy.dwave.net	TCP
207.0.72.78	207.0.72.78	TCP
207.0.112.10	207.0.112.10	TCP
207.0.119.122	mail.swaggy.com	TCP
207.0.124.132	207.0.124.132	TCP
207.0.124.133	207.0.124.133	TCP
207.0.140.3	207.0.140.3	TCP & UDP
207.0.167.206	www.casi400.com	TCP & UDP
207.0.167.213	207.0.167.213	TCP & UDP
207.0.167.218	calvin.kerasotes.com	TCP & UDP
207.0.168.194	207.0.168.194	TCP
207.0.169.18	207.0.169.18	TCP
207.0.173.51	pm1-51.akr.infi.net	TCP & UDP
208.142.100.99	208.142.100.99	TCP

208.142.121.2
208.142.121.2
TCP
208.142.130.67
208.142.130.67
TCP
208.142.141.51
208.142.141.51
TCP
208.142.143.56
208.142.143.56
TCP
208.142.143.117
pc04-santiago.mozcom.com
TCP
208.142.144.92
208.142.144.92
TCP
208.142.146.20
208.142.146.20
TCP
208.142.147.10
ppp05-davao.mozcom.com
TCP
208.142.147.47
ppp42-davao.mozcom.com
TCP
208.142.148.6
208.142.148.6
TCP
208.142.150.102
sti.edu.ph
TCP
208.142.151.195
ppp18-iloilo.mozcom.com
TCP
208.142.161.14
208.142.161.14
TCP & UDP
208.142.161.18
208.142.161.18 TCP
208.142.161.111
208.142.161.111
TCP & UDP
208.142.161.120
208.142.161.120
TCP
208.142.161.176
p48.mb03.psg.skyinet.net
TCP & UDP
208.142.161.179
p51.mb03.psg.skyinet.net
TCP
208.142.161.234
p42.mb04.psg.skyinet.net
TCP
208.142.164.4

```
    noc04.cbu.skyinet.net
     TCP
208.142.165.1
    p01.mb01.cbu.skyinet.net
  TCP
208.142.165.18
   p18.mb01.cbu.skyinet.net
  TCP
208.142.165.39
   p39.mb01.cbu.skyinet.net
  TCP & UDP
208.142.165.45
   p45.mb01.cbu.skyinet.net
  TCP
208.142.165.55
   p55.mb01.cbu.skyinet.net
TCP
208.142.165.78
   p14.mb02.cbu.skyinet.net
TCP
208.142.165.100   p36.mb02.cbu.skyinet.net
TCP & UDP
208.142.165.102
  p38.mb02.cbu.skyinet.net
TCP & UDP
208.142.165.103
  p39.mb02.cbu.skyinet.net
  TCP
208.142.167.99
   208.142.167.99
           TCP & UDP
208.142.175.34
 208.142.175.34
TCP
```

AD shoutz go out to Freaky, Kinslayer, The Weasel, and WeeDo, as well as to #su98, HackAddict HL, and to those still bangin' tryin to keep the Mac Underground alive...

/<n0wledge phreak? Yeah...I'm comin' back...I've got to. It's always been my opinion to teach, learn or burn...and I don't smoke...err...or something...anyway... so as to why I've

been away so long, I've been in transition....literally. From Colorado to New York ;p Talk about culture shock! You mean there are no Mountains in Brooklyn??? lol...Not even Mt. Vernon???

shrug Anyway, the system will be up by the time this document is wide spread, as will the web page...so hit me up.

/<n0wledge phreak www -=- http://www.k0p.com
/<n0wledge phreak FC -=- k0p.com
oleBuzzard's E-mail -=- admin@k0p.com