

**Modem Security
Dial-out Demonstration**

The logo for Xiscan, featuring a stylized 'X' shape formed by two curved lines, with the word 'iscan' in a bold, sans-serif font to its right.

iscan

Copyright © 2001 - 2004 Xiscan® Limited

Modem Security Dial-out Demonstration

Xiscan

Demonstrate what a firewall gives you...

...that a modem takes away

Compare external visibility when connecting to the Internet:

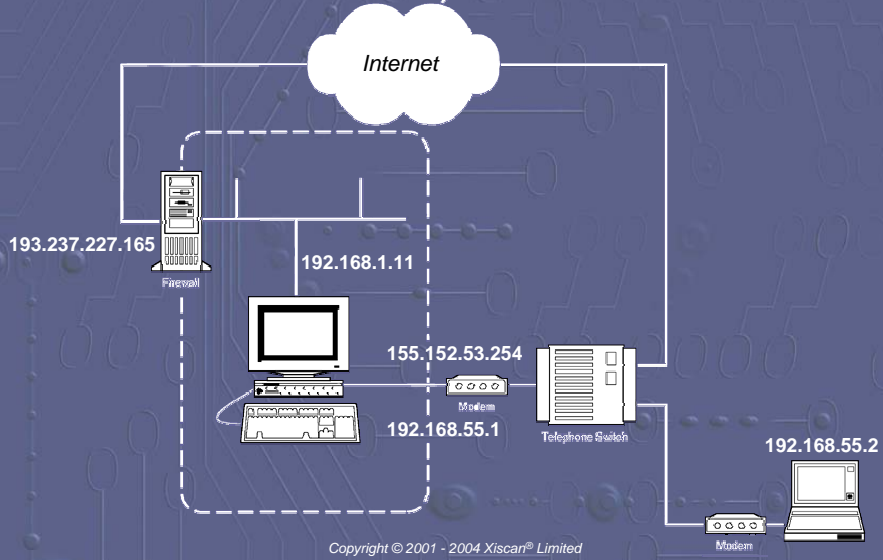
- via a firewall
- via a direct dial-out connection

Copyright © 2001 - 2004 Xiscan® Limited

Dial-out Demonstration: Environment

grc.com

Xiscan



Dial-out Demonstration: Terminology

Xiscan

Port

An agreed, unique number used as the basis to identify and communicate with a running program
(e.g. *http runs on port 80*)

Probe

An interrogation process to determine the programs running on a system (by identifying 'open' ports)

NetBios/NetBEUI

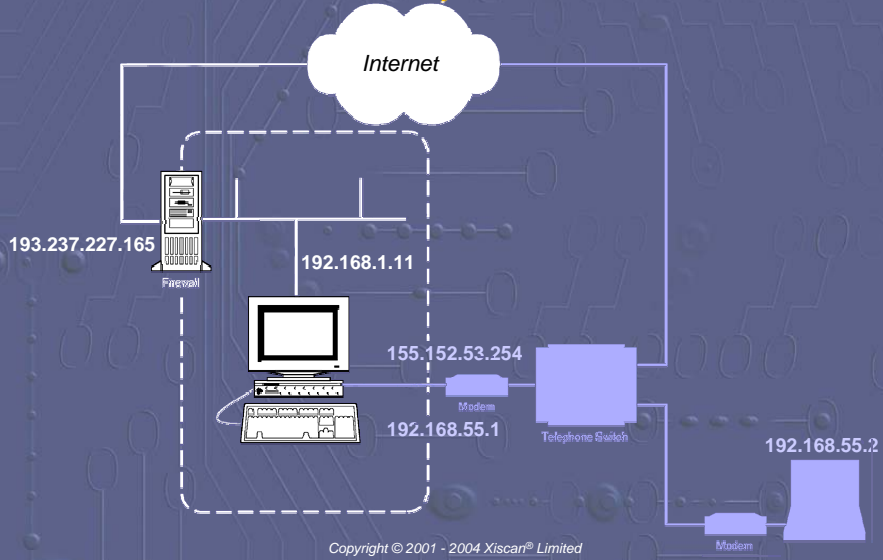
Networking services, often used as a means of sharing resources (such as printers, or disks or folders).

Copyright © 2001 - 2004 Xiscan® Limited

Internet Access via Firewall

grc.com

Xiscan



Copyright © 2001 - 2004 Xiscan® Limited

Connection through the firewall...

The screenshot shows the Shields UP! Internet Connection Security Analysis page. The browser title is "Shields UP! - Internet Connection Security Analysis - Netscape". The address bar shows the file path: file:///F:/Seminar/firewall/Shields%20UP.htm. The page features the Shields UP! logo and the text "Internet Connection Security for Windows Users by Steve Gibson, Gibson Research Corporation". The main heading reads "Shields UP! is checking YOUR computer's Internet connection security . . . currently located at IP:". Below this, the IP address "193.237.227.165" is displayed in a green box. A "Please Stand By..." message is shown. The page lists three items:

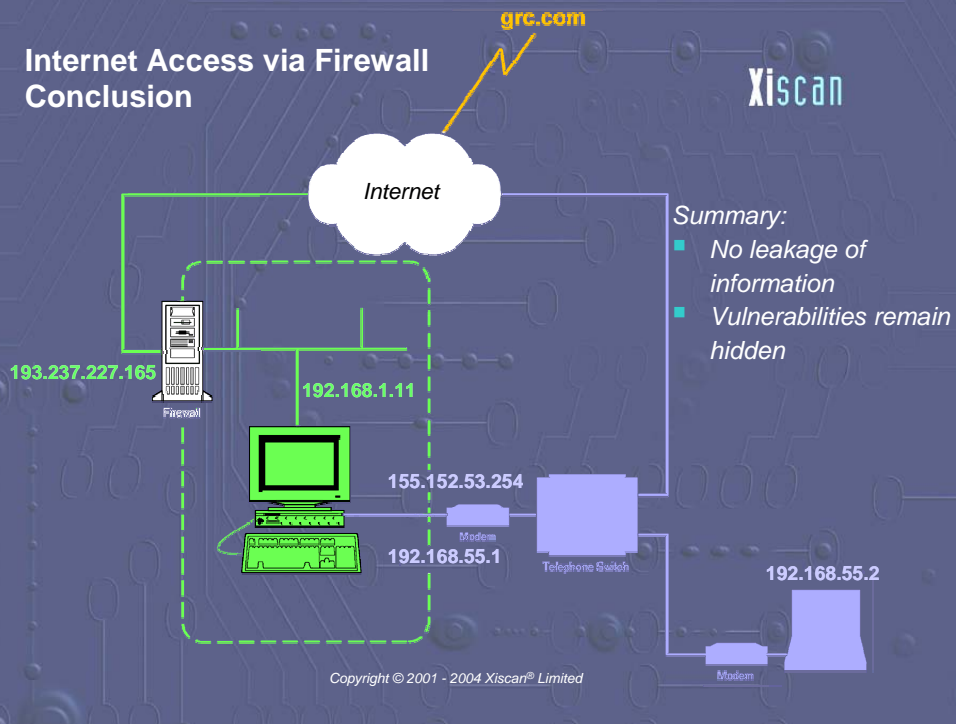
- 1 Attempting connection to your computer. . .**
Shields UP! is now attempting to contact the **Hidden Internet Server** within your PC. It is likely that no one has told you that your own personal computer may now be functioning as an **Internet Server** with neither your knowledge nor your permission. And that it may be serving up all or many of your personal files for reading, writing, modification and even deletion by anyone, anywhere, on the Internet!
Please Note: On highly secure systems this may take up to one minute. . .
- 2 Your Internet port 139 does not appear to exist!**
One or more ports on this system are operating in FULL STEALTH MODE! Standard Internet behavior requires port connection attempts to be answered with a success or refusal response. Therefore, only an attempt to connect to a nonexistent computer results in no response of either kind. **But YOUR computer has DELIBERATELY CHOSEN NOT TO RESPOND** (that's very cool!) which represents advanced computer and port stealthing capabilities. A machine configured in this fashion is well hardened to Internet NetBIOS attack and intrusion.
- 3 Unable to connect with NetBIOS to your computer.**
All attempts to get **any** information from your computer have **FAILED**. (This is **very** uncommon for a Windows networking-based PC.) Relative to vulnerabilities from Windows networking, this computer appears to be **VERY SECURE** since it is **NOT exposing ANY** of its internal NetBIOS networking protocol over the Internet.

The screenshot shows the Shields UP! Port Probe page. The browser title is "Shields UP! - Port Probe - Netscape". The address bar shows the file path: file:///F:/Seminar/firewall/Shields UP Port Probe.htm. The page features the "Port Probe" logo and the text "Internet Connection Security for Windows Users by Steve Gibson, Gibson Research Corporation". The main heading reads "Quickly Check for Connectable Listening Internet Ports". Below this, a paragraph explains that Port Probe attempts to establish standard TCP/IP (Internet) connections on a handful of standard, well-known, and often vulnerable Internet service ports on YOUR computer. Since this is being done from our server, successful connections demonstrate which of your ports are "open" and actively soliciting connections from passing Internet port scanners. The IP address "193.237.227.165" is displayed in a green box. Below the IP, it says "Is now being probed. Please stand by...". A table shows the results of the port probe:

Port	Service	Status	Security Implications
21	FTP	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
23	Telnet	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
25	SMTP	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
79	Finger	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
80	HTTP	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
110	POP3	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
113	IDENT	Closed	Your computer has responded that this port exists but is currently closed to connections.
139	Net BIOS	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!

Internet Access via Firewall Conclusion

Xiscan



Summary:

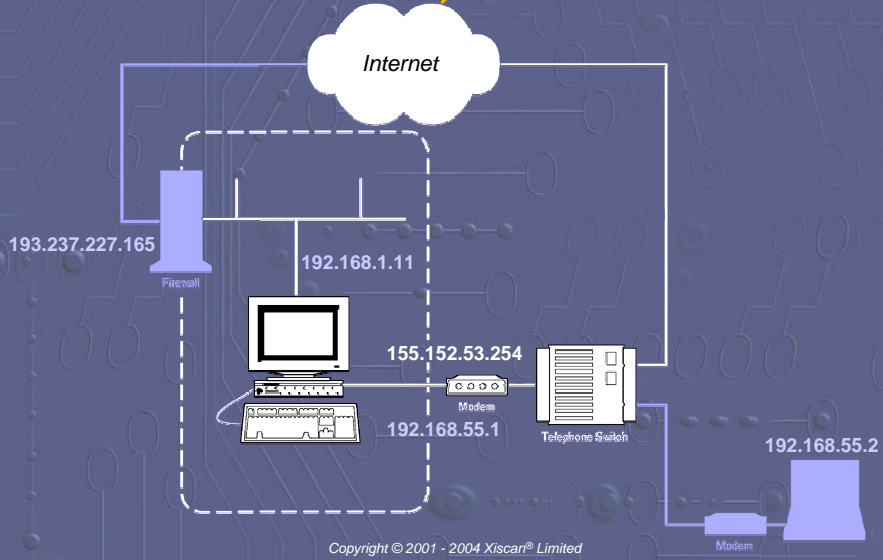
- No leakage of information
- Vulnerabilities remain hidden

Copyright © 2001 - 2004 Xiscan® Limited

Internet Access via Dial-out

grc.com

Xiscan



Copyright © 2001 - 2004 Xiscan® Limited

Connection through a dial-out connection:

Shields UP! - Internet Connection Security Analysis - Netscape

Location: file:///F:/Seminar/nofirewall/Shields UP Internet Connection.htm

Back Forward Reload Home Search Netscape Print Security Stop

The phrase you must remember is:
"My port 139 is wide OPEN!"

- 2 Remotely connected to your NetBIOS system!**
 This computer is exposing its internal NetBIOS networking protocol over the Internet. This is called "NetBIOS over TCP/IP" or "NBT" for short. This is a security risk because it gives **anyone in the world** a point of entry to your system. Connecting to your computer is **NOT** something that anyone on the Internet should be allowed to do . . . but we've just done it! The following pages provide information about the consequences and your options for increasing your system's security.
- 3 Your computer's name is: S&MINTRANET / MegaCorp Sales & Marketing IntraS&MINTRANET.**
 This is an example of some of the information about you and your computer that is leaking out onto the Internet and is openly available to **anyone**. Such information is commonly used as a starting point for guessing your name and/or your passwords and learning more about who you are.
- 4 Your computer is exposing 3 shared resources!**
 The following 3 "shares" (file system directories or printers) are being actively exposed and advertised by the **Hidden Internet Server** now running inside your computer:

Your computer's private resources are being served up to the entire Internet by software which identifies itself as: **Microsoft Windows Network**.

- S&MINTRANET — Your User Name
- S&MINTRANET — Your Computer's Name
- SALES&MARKETING — Your Workgroup

! This resource is WIDE OPEN for access by anyone in the world!

! This resource is WIDE OPEN for access by anyone in the world!

! This resource is WIDE OPEN for access by anyone in the world!

Document Done

Shields UP! - Port Probe - Netscape

Location: file:///F:/Seminar/nofirewall/Shields UP Port Probe.htm

Back Forward Reload Home Search Netscape Print Security Stop

-Port-Probe-

Internet Connection Security for Windows Users
 by Steve Gibson, Gibson Research Corporation

Quickly Check for Connectable Listening Internet Ports

Port Probe attempts to establish standard TCP/IP (Internet) connections on a handful of standard, well-known, and often vulnerable Internet service ports on **YOUR** computer. Since this is being done from **our** server, successful connections demonstrate which of your ports are "open" and actively soliciting connections from passing Internet port scanners.

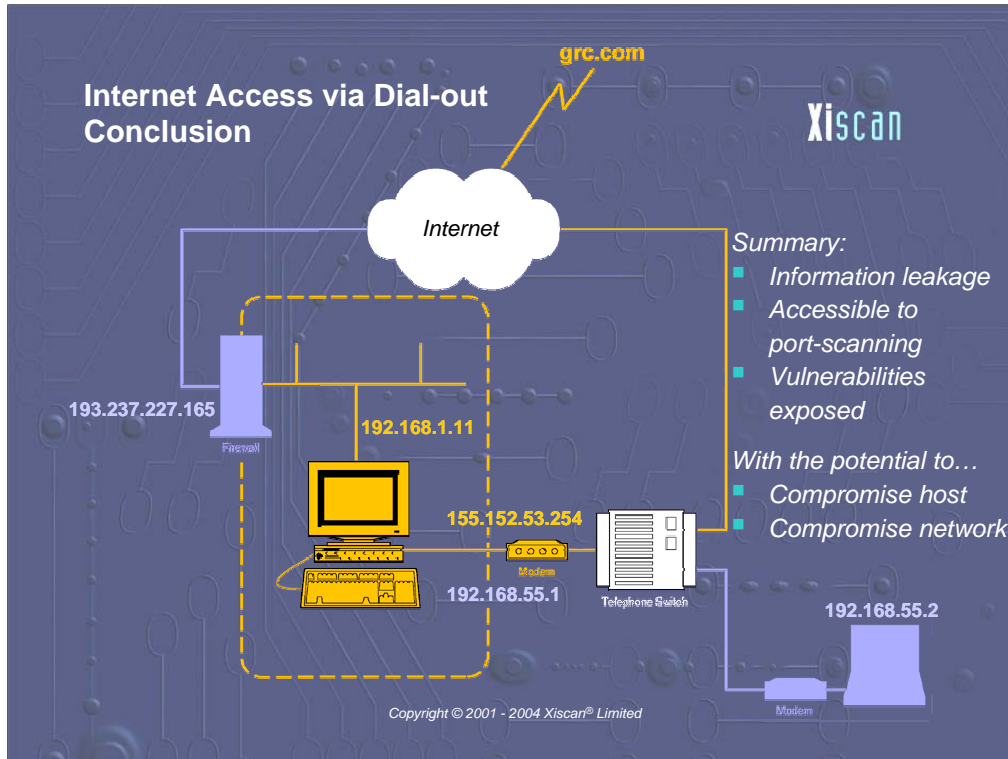
Your computer at IP:

158.152.53.244

Is now being probed. Please stand by. . .

Port	Service	Status	Security Implications
21	FTP	Closed	Your computer has responded that this port exists but is currently closed to connections.
23	Telnet	Closed	Your computer has responded that this port exists but is currently closed to connections.
25	SMTP	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
79	Finger	Closed	Your computer has responded that this port exists but is currently closed to connections.
80	HTTP	OPEN!	The web is so insecure these days that new security "exploits" are being discovered almost daily. There are many known problems with Microsoft's Personal Web Server (PWS) and its Frontpage Extensions that many people run on their personal machines. So having port 80 "open" as it is here causes intruders to wonder how much information you might be willing to give away.
110	POP3	Closed	Your computer has responded that this port exists but is currently closed to connections.
113	IDENT	Closed	Your computer has responded that this port exists but is currently closed to connections.
139	Net BIOS	OPEN!	As you probably know by now, the NetBIOS File Sharing port is the single largest security hole for networked Windows machines. The payoff from finding open Windows shares is so big that many scanners have been written just to find open ports like this one. Closing it should be a priority for

Document Done



What kind of information leaks out?:

- User name
- Computer name
- Workgroup
- Organisation
- Shared directories
- Network protocols