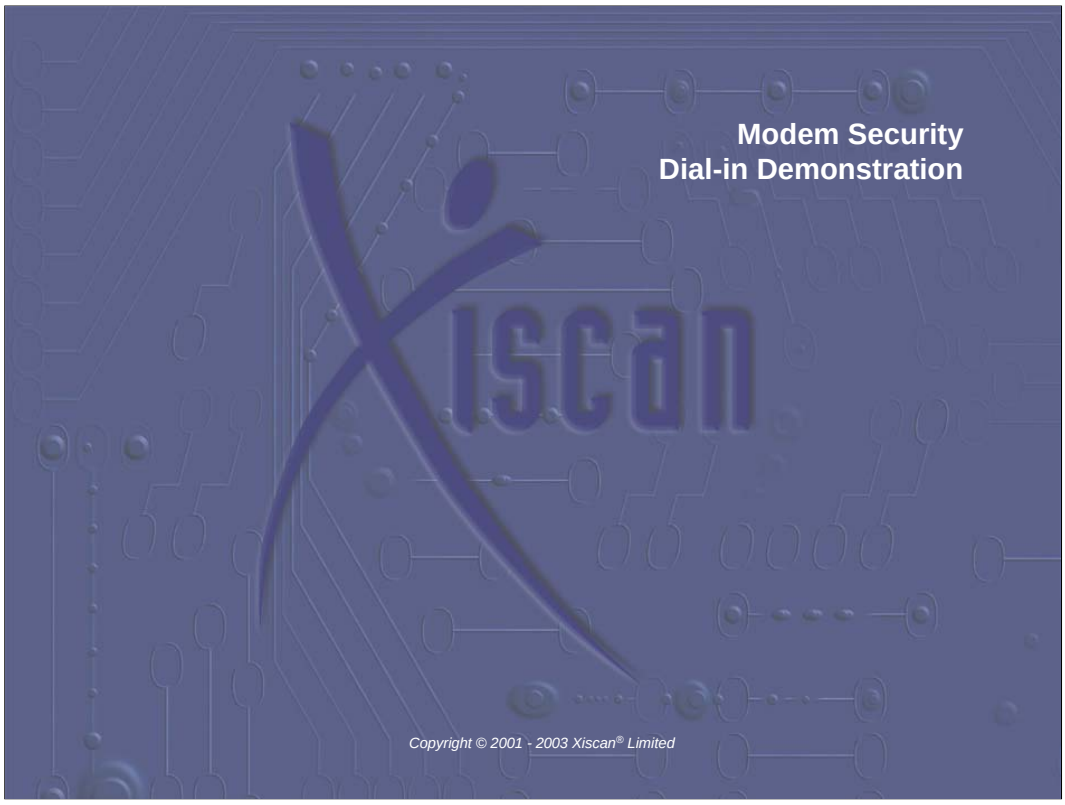
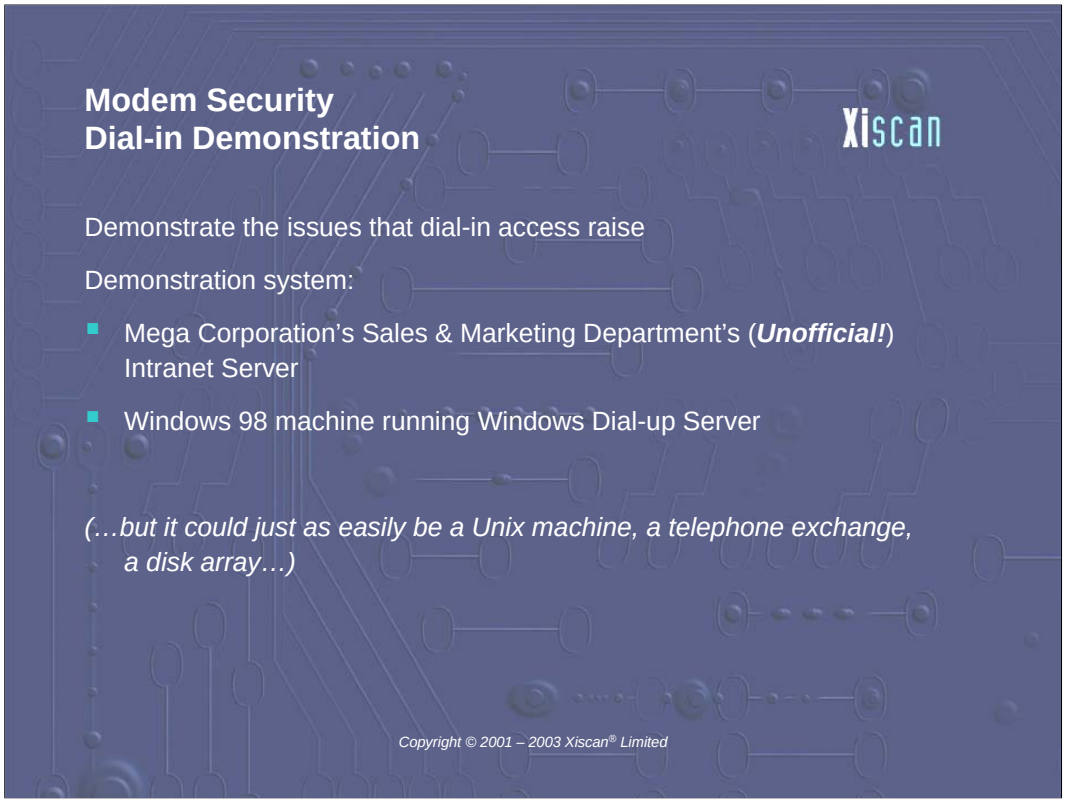
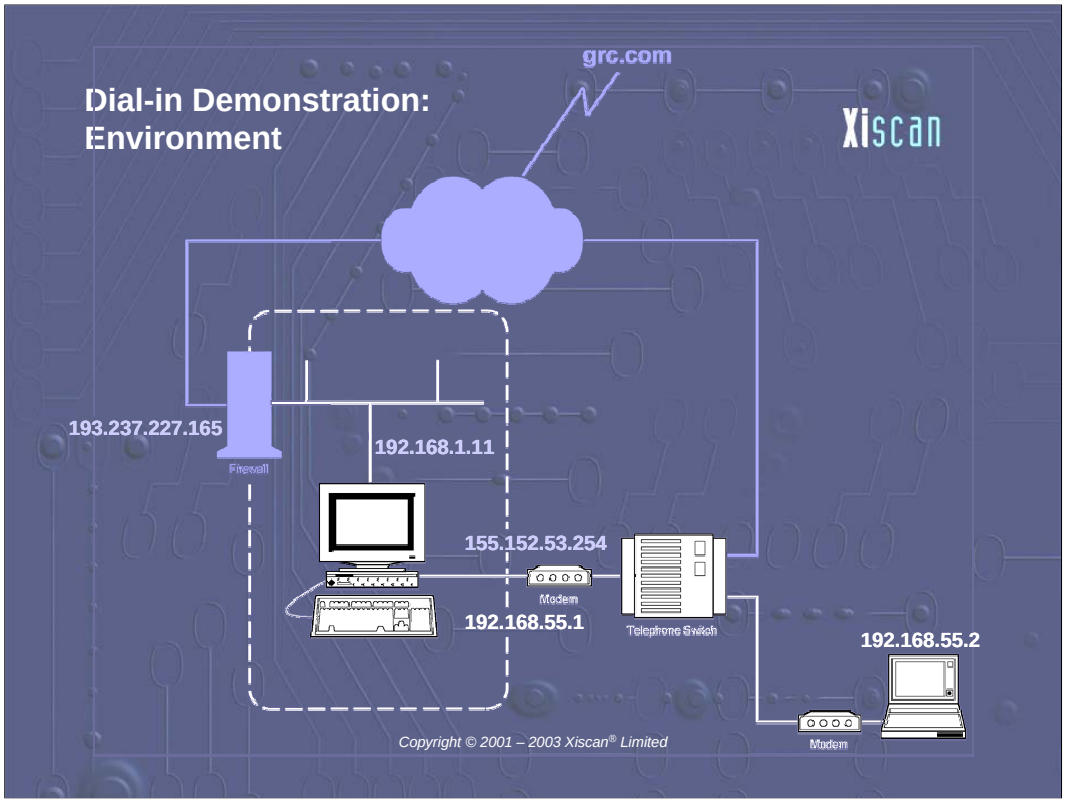

Modem Security
Dial-in Demonstration
Xiscan
Copyright © 2001 - 2003 Xiscan® Limited



With the tools provided as part of Windows, the existence of "unofficial" departmental intranet servers (configured by a local user) is a far from unusual occurrence.

… But how often have they been implemented with knowledge of best security practice?

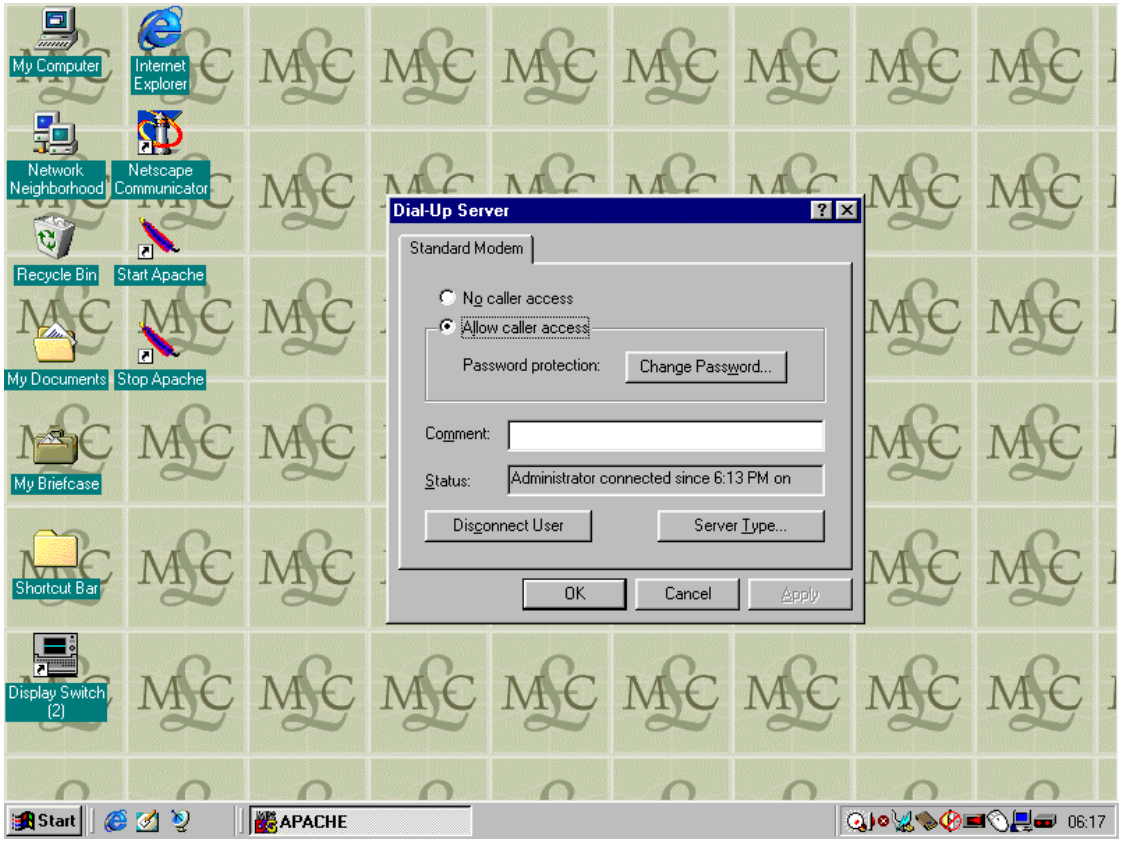

Dial-in Demonstration:
Environment
Xiscan
grc.com
193.237.227.165
Firewall
192.168.1.11
155.152.53.254
Modem
192.168.55.1
Telephone Switch
192.168.55.2
Modem
Copyright © 2001 – 2003 Xiscan® Limited

Dial-in Demonstration

Dial-inDemonstration

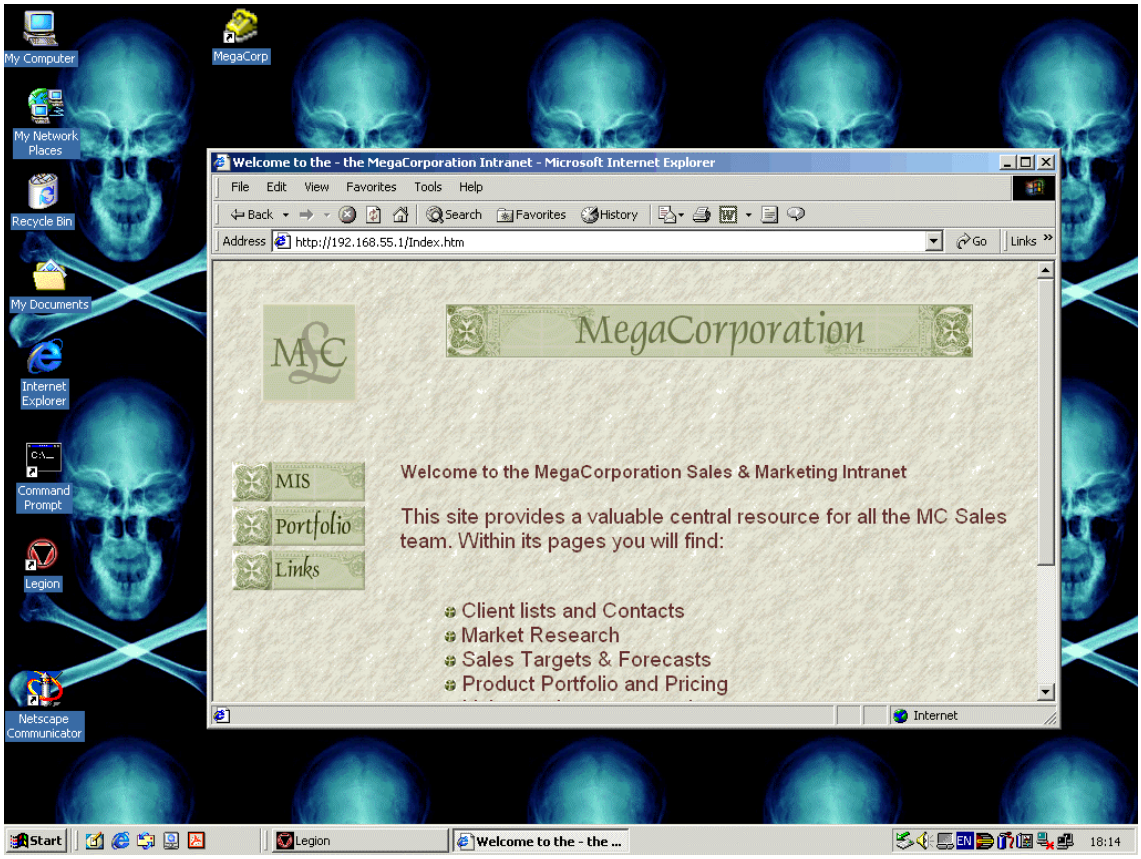
The Mega Corporation (Unofficial) S&M Intranet

Now running dial-up server – with a connection coming in through a dial-in connection from our hacker…

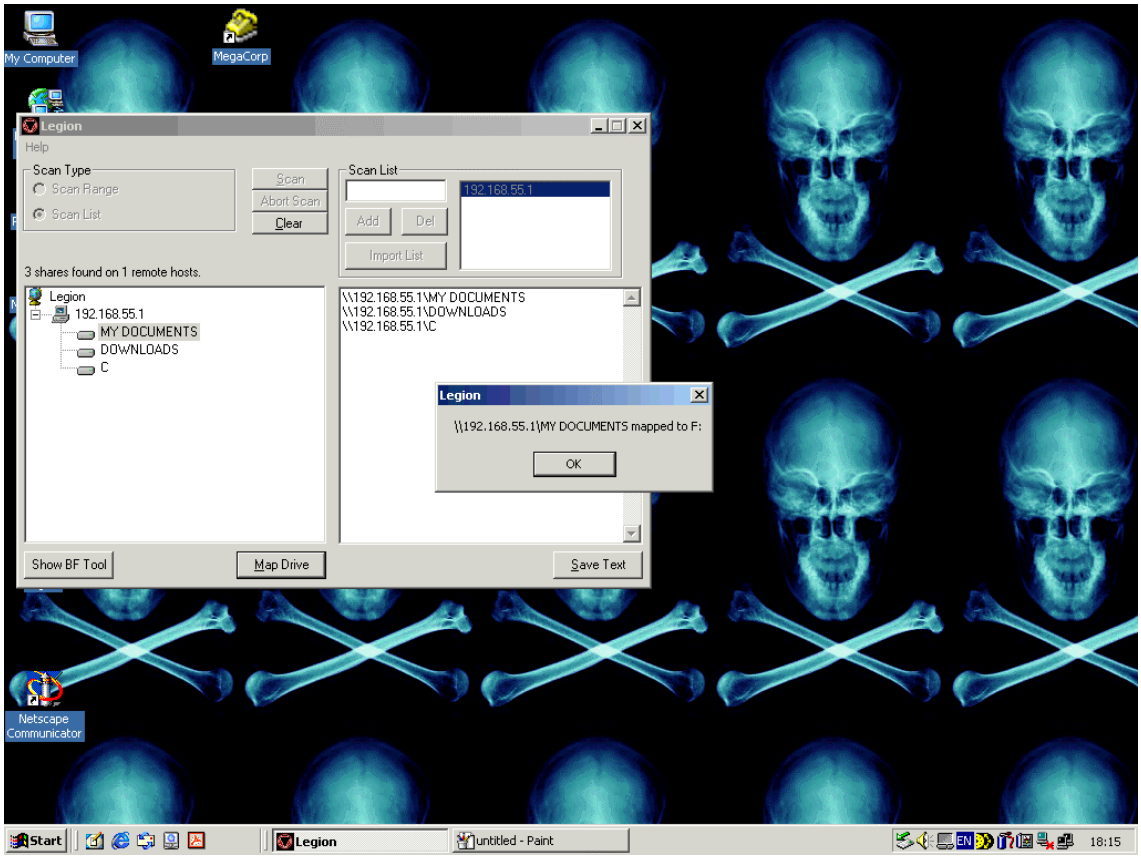


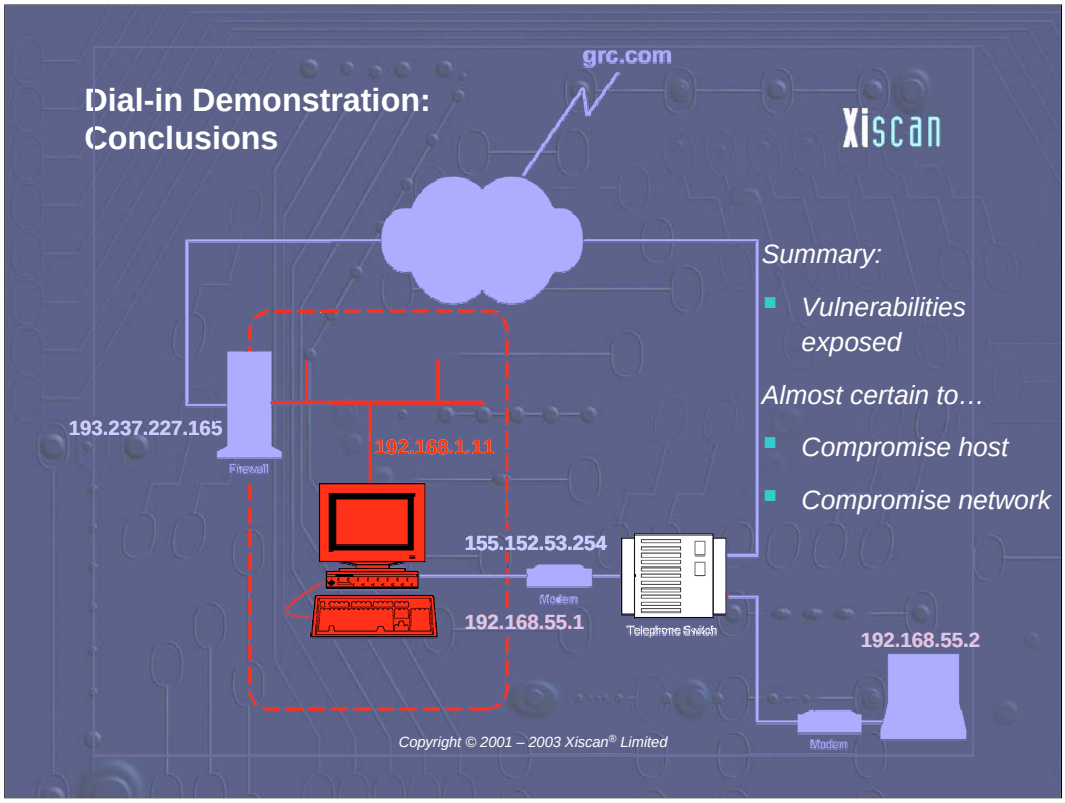
…Now what we can see from the hacker's machine ***(solely through the dial-in connection)***

We can view the Mega Corporation website…



*…and we can not only see the shared directories…****we can access them!***




Dial-in Demonstration:
Conclusions
Xiscan
grc.com
Summary:
Vulnerabilities exposed
Almost certain to…
Compromise host
Compromise network
193.237.227.165
Firewall
192.168.1.11
155.152.53.254
Modem
192.168.55.1
Telephone Switch
192.168.55.2
Modem
Copyright © 2001 – 2003 Xiscan® Limited

Dial-in *v.* Dial-out Vulnerabilities

Xiscan

All of the vulnerabilities of dial-out, plus…

- *Planned* rather than *opportunistic* attack
- Easier for a hacker to target an organisation (needs only a telephone number)
- Time to exploit the system
- System can remain compromised after the hacker disconnects
- Likely to be untraceable
- Increased likelihood that this will be a business-critical machine

…And a dial-in attack is not expensive for the hacker