Wireless Weapons of Mass Destruction for Windows

Beetle
beetle@shmoo.com

The Shmoo Group
www.shmoo.com

The Shmoo Group

Introduction & Overview

- Wi-Fi Security Soapbox
- The Disproportionate Wireless IDS Money Pit
- Free Wireless Management Mechanisms?
- Client-side Defense / Awareness?
- Blah blah blah will cover the following:
  - Rogue AP Threats
  - Simple Wi-Fi Mechanics in Windows
  - Examples and Demos of nifty code / programs
  - Other new (sorta) wireless shtuff from Shmoo

The Shmoo Group

Rogue Access Points

- Traditional threats consist of:
  - Wannabe-mobile employees
  - Physical insertion for corporate espionage
- New threats, a la Airsnarf
  - Intentional rogue AP setup for snarfing info
  - Check out airsnarf.shmoo.com for more info.
- And what about new SoftAP threats?
  - We've been saying it for some time now—Wi-Fi WILL be a worm target in the future!
  - How? Via WMI probably...

The Shmoo Group

Access Point

SSID: “goodguy”

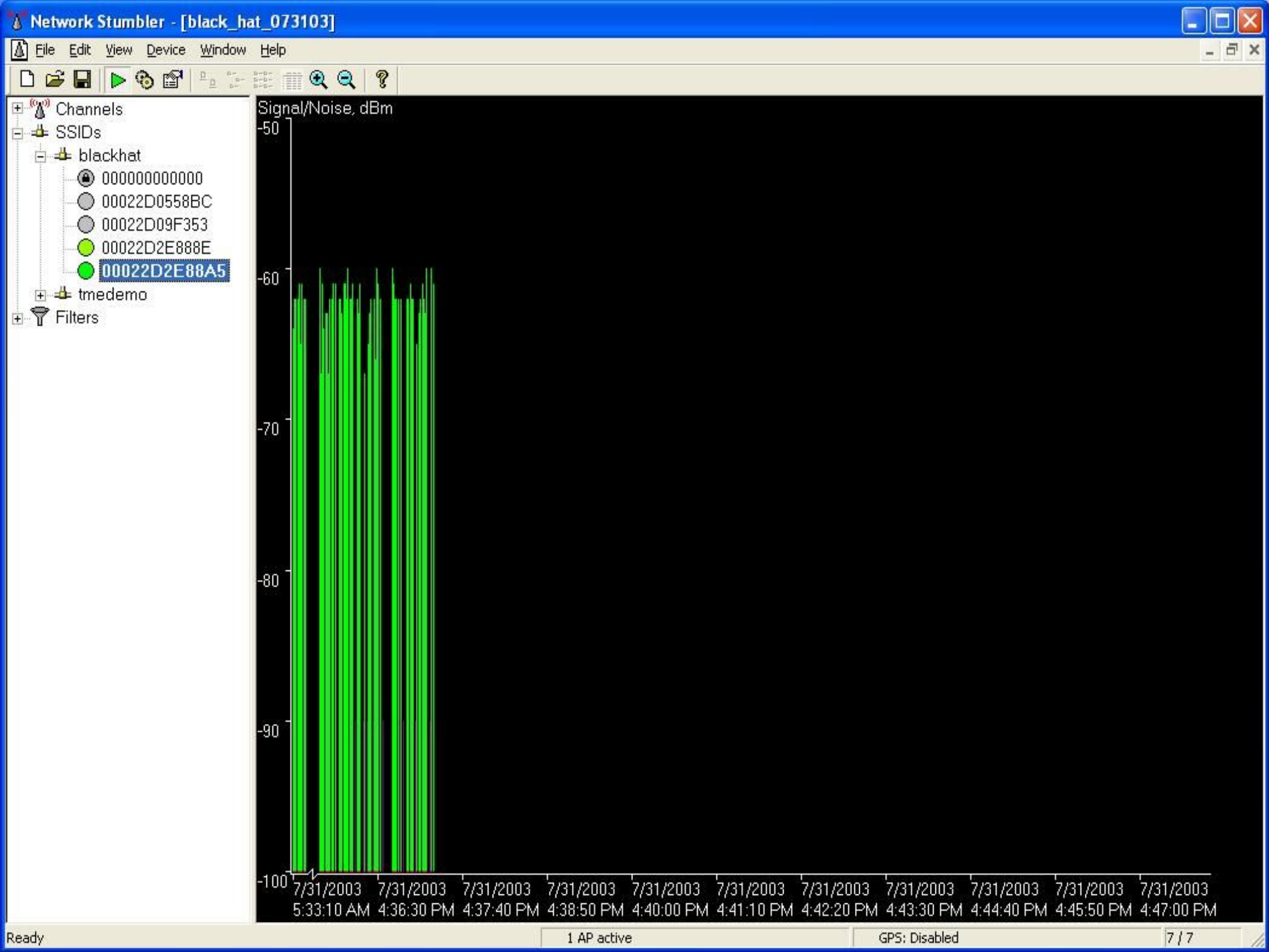
Stronger or Closer Access Point

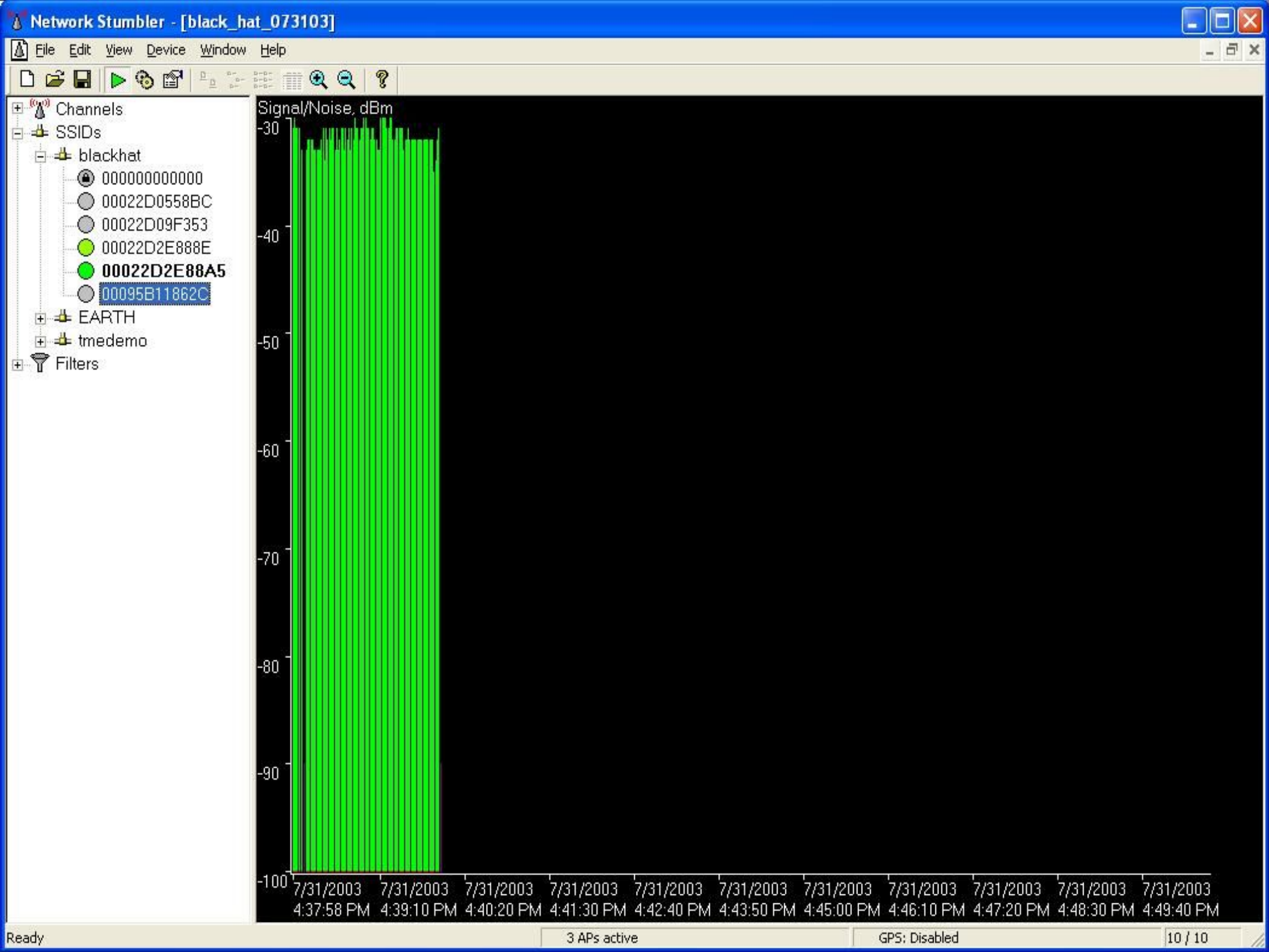
SSID: “badguy”

Wi-Fi Card

SSID: “badguy”

The Shmoo Group


Network Stumbler - [black_hat_073103]
File Edit View Device Window Help
Channels
SSIDs
blackhat
000000000000
00022D0558BC
00022D09F353
00022D2E888E
00022D2E88A5
tmedemo
Filters
Signal/Noise, dBm
-50
-60
-70
-80
-90
-100
7/31/2003 5:33:10 AM
7/31/2003 4:36:30 PM
7/31/2003 4:37:40 PM
7/31/2003 4:38:50 PM
7/31/2003 4:40:00 PM
7/31/2003 4:41:10 PM
7/31/2003 4:42:20 PM
7/31/2003 4:43:30 PM
7/31/2003 4:44:40 PM
7/31/2003 4:45:50 PM
7/31/2003 4:47:00 PM
Ready
1 AP active
GPS: Disabled
7 / 7

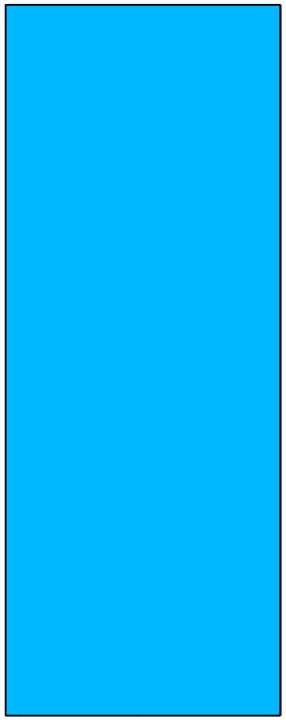

Network Stumbler - [black_hat_073103]
File Edit View Device Window Help
Channels
SSIDs
blackhat
000000000000
00022D0558BC
00022D09F353
00022D2E888E
00022D2E88A5
00095B11862C
EARTH
tmedemo
Filters
Signal/Noise, dBm
-30
-40
-50
-60
-70
-80
-90
-100
7/31/2003 4:37:58 PM
7/31/2003 4:39:10 PM
7/31/2003 4:40:20 PM
7/31/2003 4:41:30 PM
7/31/2003 4:42:40 PM
7/31/2003 4:43:50 PM
7/31/2003 4:45:00 PM
7/31/2003 4:46:10 PM
7/31/2003 4:47:20 PM
7/31/2003 4:48:30 PM
7/31/2003 4:49:40 PM
Ready
3 APs active
GPS: Disabled
10 / 10

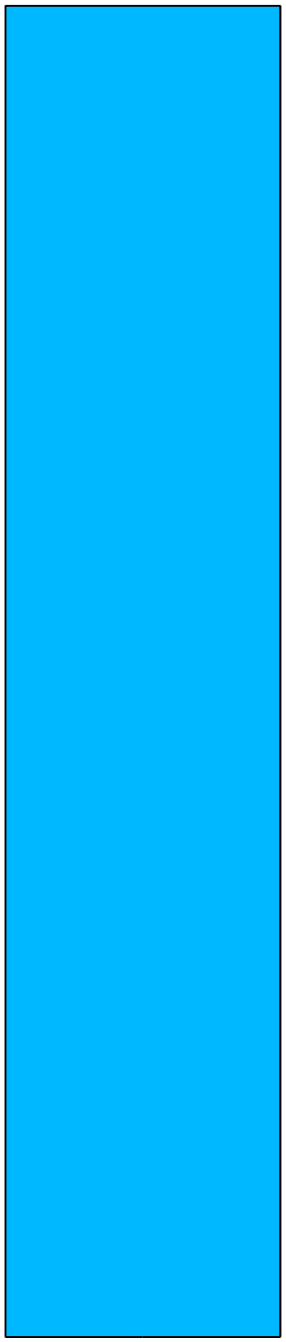
Choose your Wi-Fi weapon...

Senao Gear @
200mW
(23dBm)

Cisco Gear @
100mW
(20dBm)

Normal Gear @
25mW
(14dBm)





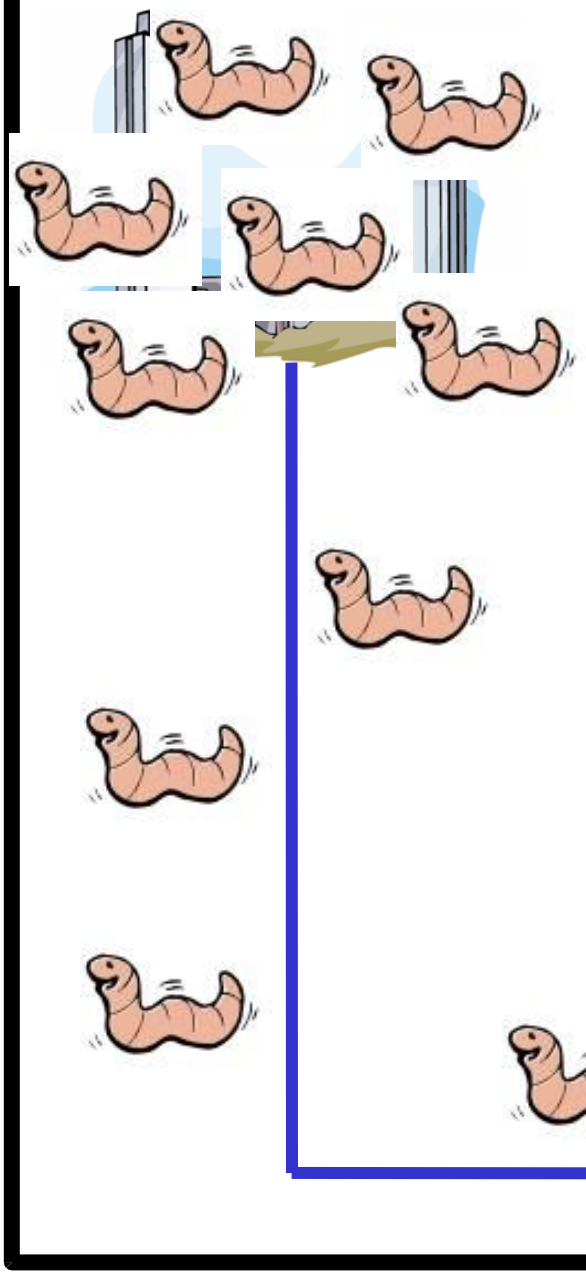
Use a 15dBd antenna with a Senao for 38dBd total...

6 WATTS!

Vs 25mW?

NO CONTEST!

The Shmoo Group



Inverse Wardriving *v.*
(gnivirdraw)

1. A rogue AP looking for “WiFi suckers”.

2. And you thought a user dual-homed with a **modem** was bad… ?

The Shmoo Group

WTF is WMI?

- Windows Management Instrumentation
  - Microsoft extension to DMTF's CIM under WBEMI
  - WTF? Ok. I'll TRY to explain.
- Whoa! What's this? NDIS?
  - NDIS management under WMI namespace
  - Cool. MSNdis_80211 stuff. Wireless.
- Nifty utilities like wbemtest & CIM Studio!
  - In Windows XP, Start, Run, wbemtest
- More info on WMI here:
  - http://msdn.microsoft.com/library/en-us/wmisdk/wmi/wmi_start_page.asp

The Shmoo Group

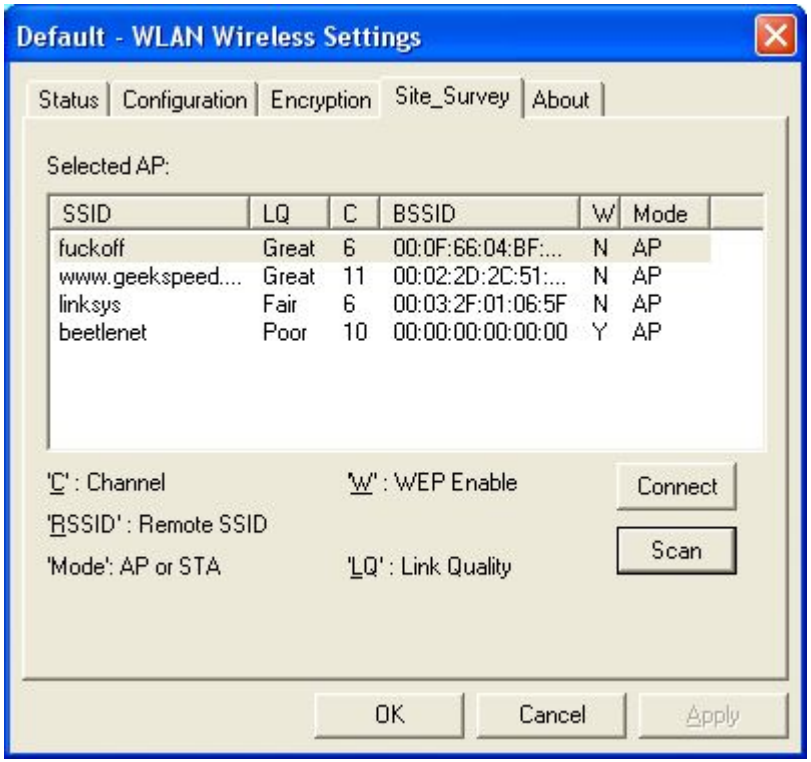
Wi-Fi via WMI

- This looks cool, but how do I sling code?
  - WQL = SQL for WMI
  - Pick namespace, make select statements, and enumerate instances or results to get WMI data
- VBScript
  - Pros: Quick to implement, interpreted so no compiler, runs on any modern Win32 OS
  - Cons: Uhh... it's VBScript.
- C#
  - Pros: Quick GUIs, registered events
  - Cons: Requires compiler, .NET downloads

The Shmoo Group

Windows = SSIDs via GUI

- It seems a GUI is needed to find a network when you're using Windows. Grrr.
  - Card utility, Windows utility, Netstumbler
  - Like so...



The Shmoo Group

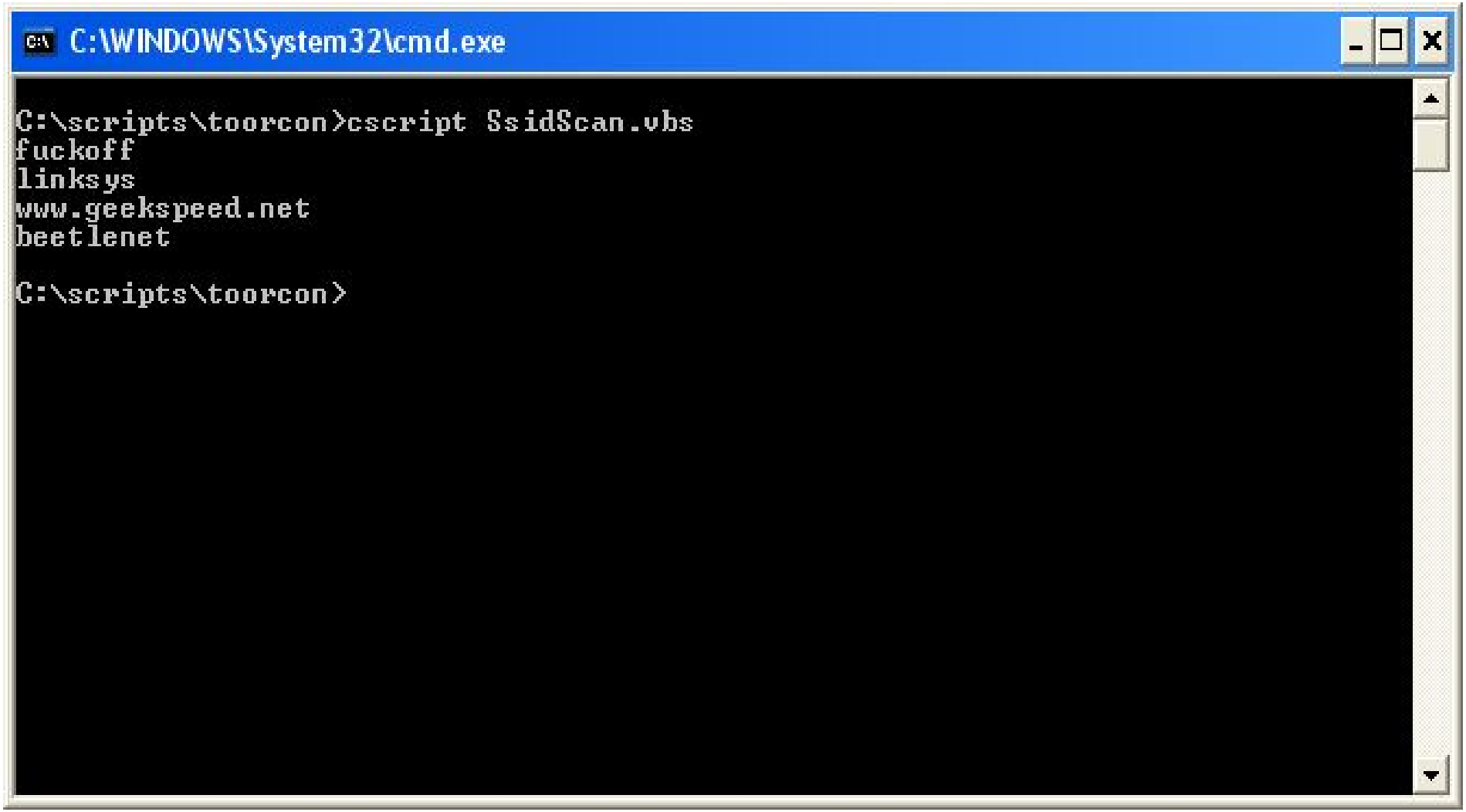
SO difficult via VBScript...

```
on error resume next
set objSWbemServices = GetObject("winmgmts:\\.\root\wmi")
set colInstances = objSwbemServices.ExecQuery("SELECT * FROM MSNDis_80211_BSSIList")
for each obj in colInstances
	if left(obj.InstanceName, 4) <> "WAN " and right(obj.InstanceName, 8) <> "Miniport" then
		for each rawssid in obj.Ndis80211BSSIList
			ssid = ""
			for i=0 to ubound(rawssid.Ndis80211SSid)
				decval = rawssid.Ndis80211Ssid(i)
				if (decval > 31 AND decval < 127) then
					ssid = ssid & Chr(decval)
				end if
			next
			wscript.echo ssid
		next
	end if
next
```

The Shmoo Group

OK. Maybe not. ;)

SsidScan.vbs



The Shmoo Group

Iwconfig for XP

- Started out as a VBScript, ended up C#.
- Code is very sequential. And shitty.
- Allows for displaying of implemented MSNdis_80211 crap in root\WMI namespace.
- Can also change SSID from the cmd prompt!
- Works OK with a Senao 2511 200mW.
- Works not so OK with most everything else.
- YMMV. BIGtime.

The Shmoo Group

iwconfig.vbs

```
C:\WINDOWS\system32\cmd.exe
C:\scripts\toorcon>cscript iwconfig.vbs
iwconfig XP
0.1
An iwconfig-like command for Windows XP using WMI.  Displays stats only, for now
.
Beetle <beetle@shmoo.com>

Usage: cscript iwconfig.vbs [adapter]

wlan0  D-Link AirPlus DWL-520+ Wireless PCI Adapter
wlan1  D-Link AirPlus DWL-520+ Wireless PCI Adapter - Deterministic Network Enha
ncer Miniport
wlan2  D-Link AirPlus DWL-520+ Wireless PCI Adapter - Packet Scheduler Miniport

C:\scripts\toorcon>cscript iwconfig.vbs wlan0
wlan0  D-Link AirPlus DWL-520+ Wireless PCI Adapter
       ESSID:"beetlenet"  Nickname:"FLYNT"
       Mode:Infrastructure  Channel:11  Cell: 00:09:5B:AE:D4:E8
       Bit Rate:11Mb/s  Sensitivity:N/A
       RTS thr:4096  Fragment thr:4095
       Power Management:off
       Link Quality:N/A  Signal level:0dBm  Noise level:N/A
       Rx invalid nwid:N/A  invalid crypt:N/A  invalid misc:N/A

C:\scripts\toorcon>_
```

The Shmoo Group

iwconfig.exe

C:\WINDOWS\System32\cmd.exe

```
C:\>iwconfig
iwconfig XP
0.2
An iwconfig-like command for Windows XP.
Beetle <beetle@shmoo.com>
Usage: iwconfig <adapter> [essid <SSID>]

wlan0 IEEE 802.11b WLAN network adaptor PC Card
wlan1 IEEE 802.11b WLAN network adaptor PC Card - Deterministic Network Enhancer
 Miniport
wlan2 IEEE 802.11b WLAN network adaptor PC Card - Packet Scheduler Miniport

C:\>iwconfig wlan0 essid beetlenet

C:\>iwconfig wlan0
wlan0  IEEE 802.11b WLAN network adaptor PC Card
       ESSID:beetlenet  Nickname:SCULLY
       Mode:Infrastructure  Channel:10  BSSID:00:09:5B:AE:D4:E8
       Bit Rate:11Mb/s  Sensitivity:N/A
       RTS thr:  Fragment thr:
       Power Management:on
       Link Quality:N/A  Signal level:-66dBm  Noise level:N/A
       Rx invalid nwid:  invalid crypt:  invalid misc:

C:\>
```

The Shmoo Group

More WMI w/ VBScript

- Continuously query local signal? Cool, but I can do that with my card's utility.
- Continuously query signal of REMOTE workstation though? Darn, I can't do that with my my card's utility. WMI rocks.
- Have access to remote system? Use WMI to query:
  - Received signal strength, current BSSID, available SSIDs, etc.
- Hmmm. This could be FUN.

The Shmoo Group

WiFiLocalSignal.vbs

C:\WINDOWS\System32\cmd.exe - cscript WiFiLocalSignal.vbs 1

```
C:\scripts\toorcon>cscript WiFiLocalSignal.vbs
Wi-Fi Local Signal Monitor
0.1
BSSID, SSID, and RSSI monitor of local XP machine's Wi-Fi card via WMI.
Beetle <beetle@shmoo.com>

Usage: cscript WiFiLocalSignal.vbs [cardno]
1 = IEEE 802.11b WLAN network adaptor PC Card
2 = IEEE 802.11b WLAN network adaptor PC Card - Deterministic Network Enhancer M
iniport
3 = IEEE 802.11b WLAN network adaptor PC Card - Packet Scheduler Miniport

C:\scripts\toorcon>cscript WiFiLocalSignal.vbs 1
Wi-Fi Local Signal Monitor
0.1
BSSID, SSID, and RSSI monitor of local XP machine's Wi-Fi card via WMI.
Beetle <beetle@shmoo.com>

Using IEEE 802.11b WLAN network adaptor PC Card

BSSID: 00:09:5B:AE:D4:E8  SSID: beetlenet  RSSI: -30dB
BSSID: 00:09:5B:AE:D4:E8  SSID: beetlenet  RSSI: -38dB
BSSID: 00:09:5B:AE:D4:E8  SSID: beetlenet  RSSI: -35dB
```

The Shmoo Group

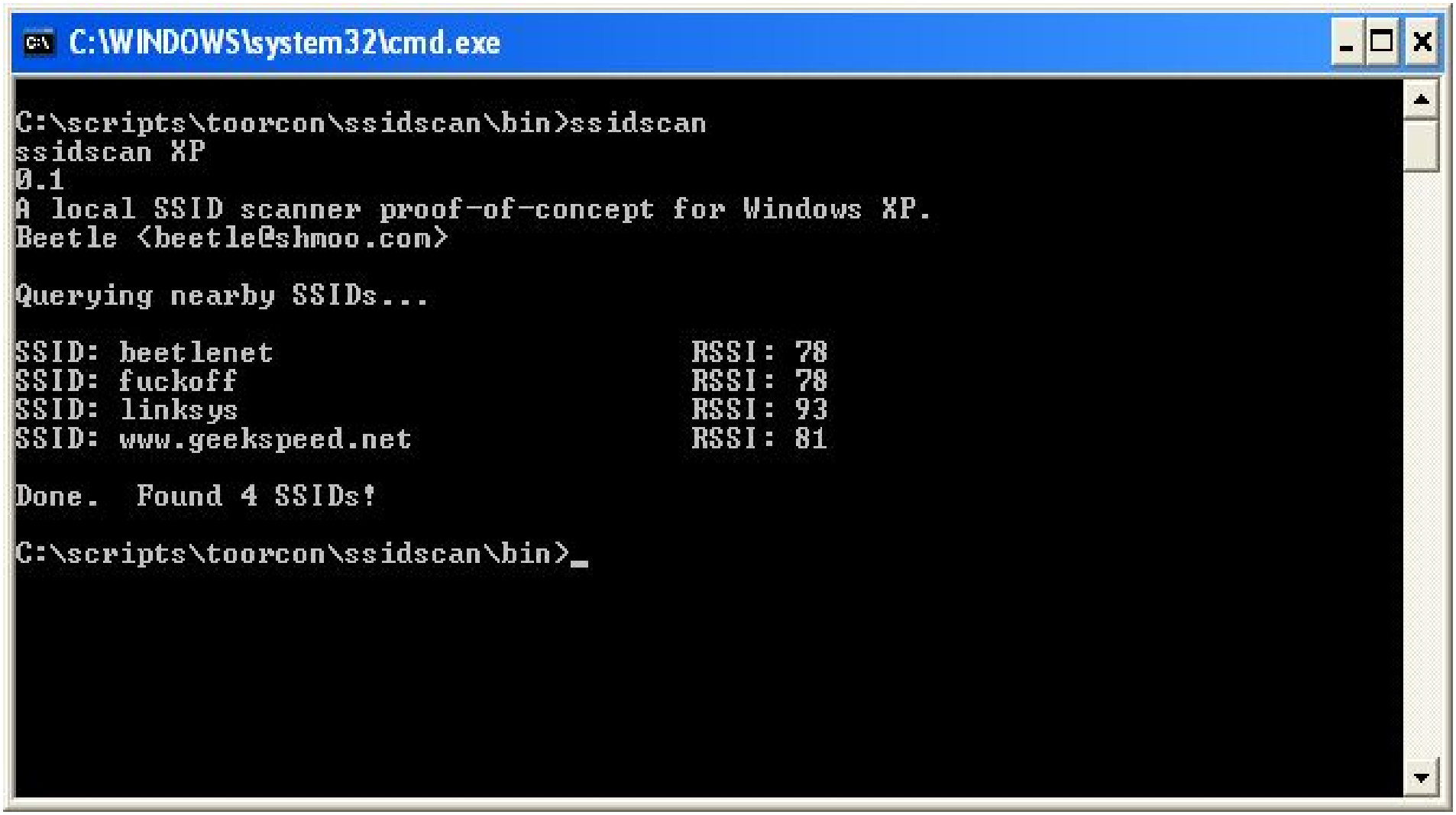
WiFiRemoteSignal.vbs

C:\WINDOWS\system32\cmd.exe - cscript WiFiRemoteSignal.vbs 1

```
C:\scripts\toorcon>cscript WiFiRemoteSignal.vbs
Wi-Fi Remote Signal Monitor
0.1
BSSID, SSID, and RSSI monitor of a remote XP machine's Wi-Fi card via WMI.
Beetle <beetle@shmoo.com>

Usage: cscript WiFiRemoteSignal.vbs [cardno]
1  = IEEE 802.11b WLAN network adaptor PC Card
2  = IEEE 802.11b WLAN network adaptor PC Card - Deterministic Network Enhancer M
iniport
3  = IEEE 802.11b WLAN network adaptor PC Card - Packet Scheduler Miniport

C:\scripts\toorcon>cscript WiFiRemoteSignal.vbs 1
Wi-Fi Remote Signal Monitor
0.1
BSSID, SSID, and RSSI monitor of a remote XP machine's Wi-Fi card via WMI.
Beetle <beetle@shmoo.com>

Using IEEE 802.11b WLAN network adaptor PC Card

BSSID: 00:09:5B:AE:D4:E8  SSID: beetlenet  RSSI: -28dB
BSSID: 00:09:5B:AE:D4:E8  SSID: beetlenet  RSSI: -27dB
BSSID: 00:09:5B:AE:D4:E8  SSID: beetlenet  RSSI: -26dB
```

The Shmoo Group

ssidscan.exe



The Shmoo Group

ssidpeek.exe

C:\WINDOWS\System32\cmd.exe

```
C:\scripts\toorcon\ssidpeek\bin>ssidpeek
ssidpeek XP
0.1
A remote SSID scanner proof-of-concept for Windows XP.
Beetle <beetle@shmoo.com>

Usage: ssidpeek <hostname or IP> <username> <password>


C:\scripts\toorcon\ssidpeek\bin>ssidpeek 192.168.10.2 beetle sillypassword
ssidpeek XP
0.1
A remote SSID scanner proof-of-concept for Windows XP.
Beetle <beetle@shmoo.com>

Querying SSIDs for 192.168.10.2...

SSID: beetlenet                          RSSI: 80
SSID: fuckoff                            RSSI: 73
SSID: linksys                            RSSI: 92
SSID: www.geekspeed.net                  RSSI: 80

Done.  Found 4 SSIDs at 192.168.10.2!

C:\scripts\toorcon\ssidpeek\bin>
```

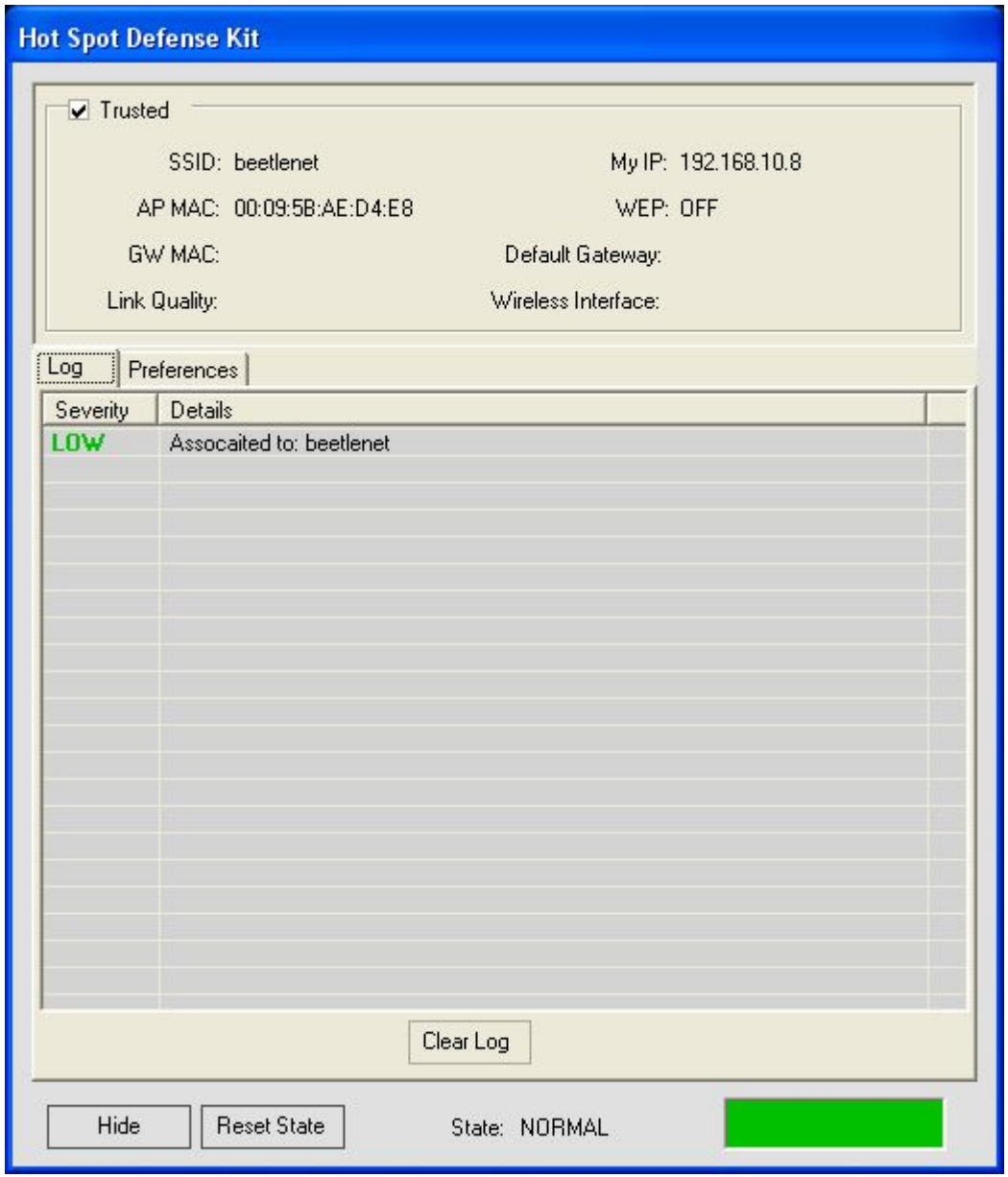
The Shmoo Group

HotspotDK for XP

- GREAT example of what you can REALLY do Wi-Fi programming-wise with WMI.
- A full-on Windows implementation of the client-side wireless IDS, HotspotDK, for detecting rogue AP activity.
- Previously only available for OS X.
- Written in C# one evening by Windows programming wizard Scott Tenaglia, a.k.a. “Intern”, intern@geekspeed.net
- Requires .NET Framework 1.1
- Download at airsnarf.shmoo.com

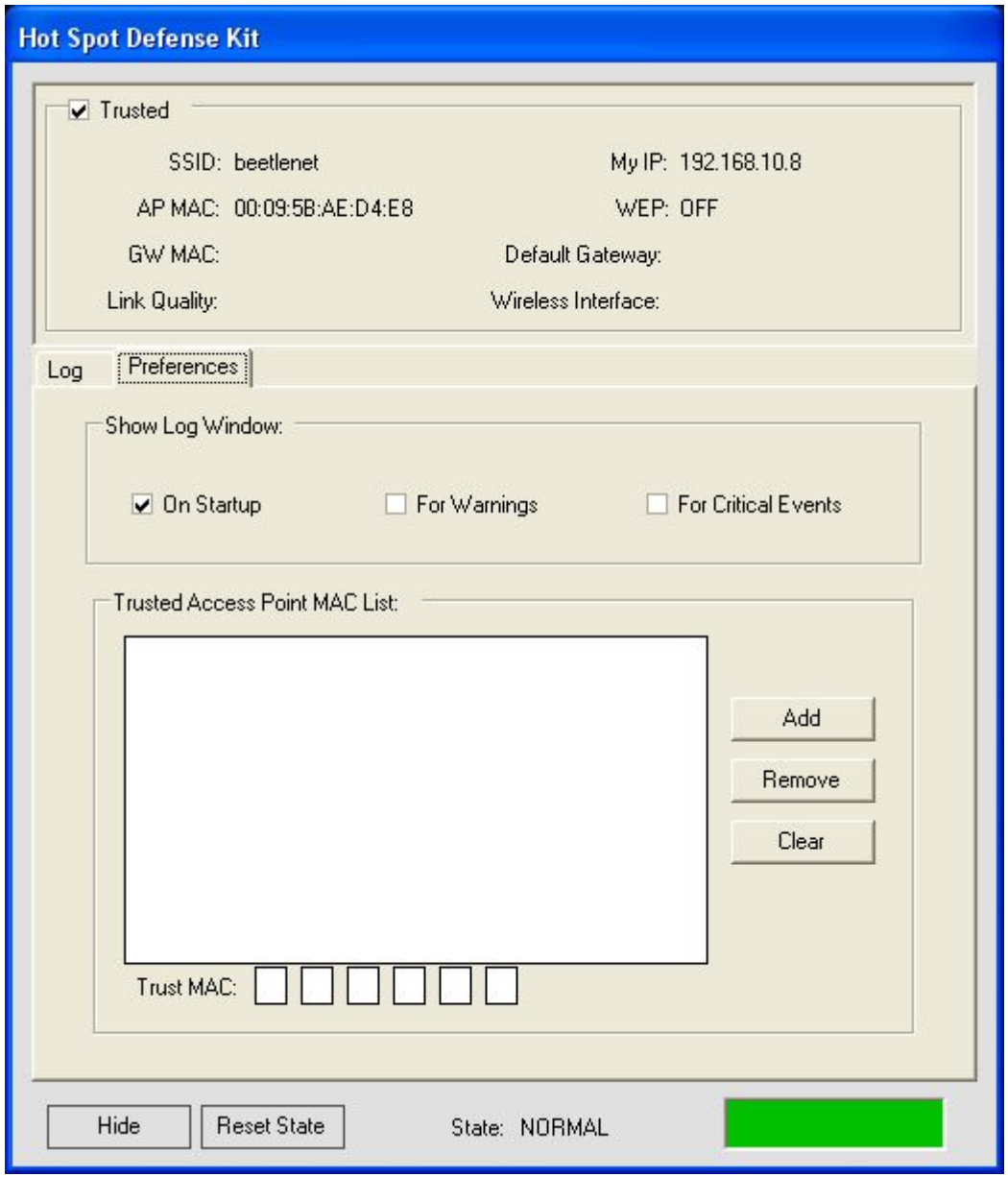
The Shmoo Group

HotspotDK



The Shmoo Group

HotspotDK



The Shmoo Group

Managing Wi-Fi at Work

- Windows Server 2003 has some interesting wireless management via Group Policy.
- But it would be nice to know when folks have wireless enabled WHILE connected to the Intranet LAN.
- A simple query for active wireless adapters should suffice.
  - Needs to be made in conjunction with checking for LAN link status.
- Make it targetted for indivdual suspects or search the domain. But for now...

The Shmoo Group

WiFiMultiHome.vbs

C:\WINDOWS\System32\cmd.exe

```
C:\scripts\toorcon>cscript WiFiMultiHome.vbs
Wi-Fi Multi-Homed Checker
0.1
Example script to locally check for multi-homed condition, including Wi-Fi.
Beetle <beetle@shmoo.com>


3Com 3C920 Integrated Fast Ethernet Controller (3C905C-TX Compatible), 100Mbps
This adapter is disconnected.

IEEE 802.11b WLAN network adaptor PC Card, 11Mbps
This adapter is connected.
This adapter is wireless.


Found wireless, but we're not connected to multiple networks.  No biggie.

C:\scripts\toorcon>_
```

The Shmoo Group

When multi-homed...ALERT!

```
C:\WINDOWS\System32\cmd.exe

C:\scripts\toorcon>cscript WiFiMultiHome.vbs
Wi-Fi Multi-Homed Checker
0.1
Example script to locally check for multi-homed condition, including Wi-Fi.
Beetle <beetle@shmoo.com>


3Com 3C920 Integrated Fast Ethernet Controller (3C905C-TX Compatible), 100Mbps
This adapter is connected.

IEEE 802.11b WLAN network adaptor PC Card, 11Mbps
This adapter is connected.
This adapter is wireless.


Connected to 2 networks--1 wireless!  Ack!

C:\scripts\toorcon>
```

The Shmoo Group

WiFiMultiHomeLogon.vbs

C:\WINDOWS\System32\cmd.exe

```
C:\scripts\toorcon>cscript WiFiMultiHomeLogon.vbs
Wi-Fi Multi-Homed Checker Logon Script
0.1
Example logon script that checks for multi-homed condition, including Wi-Fi,
 and post results to a central server / share.
Beetle <beetle@shmoo.com>

Gathering information from SCULLY (192.168.10.6)...
Done.
Sending information...
Done.

C:\scripts\toorcon>_
```

The Shmoo Group

Sample Logged Output

Information for SCULLY (192.168.10.6) obtained 9/22/2004 4:10:50 PM:

3Com 3C920 Integrated Fast Ethernet Controller (3C905C-TX Compatible), 100Mbps
MAC: 00:0B:DB:1D:A6:BC
This adapter is disconnected.

IEEE 802.11b WLAN network adaptor PC Card, 11Mbps
MAC: 00:02:6F:06:0B:B3
This adapter is connected.
This adapter is wireless.

Found wireless, but we're not connected to multiple networks. No biggie.

The Shmoo Group

Another example. Uh-Oh...

Information for SCULLY (192.168.10.6) obtained 9/22/2004 4:19:00 PM:

3Com 3C920 Integrated Fast Ethernet Controller (3C905C-TX Compatible), 100Mbps
MAC: 00:0B:DB:1D:A6:BC
This adapter is connected.

IEEE 802.11b WLAN network adaptor PC Card, 11Mbps
MAC: 00:02:6F:06:0B:B3
This adapter is connected.
This adapter is wireless.

Connected to 2 networks--1 wireless! Ack!

The Shmoo Group

What about Wi-Fi worms?

- That's just not possible. Is it? Maybe.
- Worms these days, in general, suck. They don't do anything INTERESTING. Own box, install backdoor, scan, rinse, repeat.
- So theoretically, in the distant future, a Wi-Fi worm would do the following after owning the box:
  - Report back current and available SSIDs
  - Set SSID in ad-hoc, client, or SoftAP mode
  - Create an alternate out-of-band network
  - Allow for inverse war-driving & Wi-Fi backdoors

The Shmoo Group

Worldwide Wardrive?

- To check with all this driving and walking around to find wireless networks.
- What we need is a SETI@home sort of app for performing a global wardrive from one location!
  - IP geolocation, SSID scanning, reports back to “mothership”, etc.
  - “War-lounging”, so to speak.
  - Whether intentional or piggy-backing with a worm, there should be a program that does this...

The Shmoo Group

WarLounge.vbs

- Proof-of-concept code that could be given out to friends or piggy-back on a worm to perform a global wardrive.
- About 40 lines of VBScript.
- Performs SSID scan, saves results, emails them to beetle@shmoo.com
  - Please change the “To:” field. Thanks. ;)
- Kinda sucks without IP geolocation.
  - Any ideas?
- Could be logon script, ASP, executable, you name it.

The Shmoo Group

A few caveats...

- XP boxen in a workgroup and not domain need to have “force guest” turned OFF.
  - XP Home boxen can't do this, I guess.
  - Do this through your local security policy.
- WMI-based wireless apps seem to work best with Windows Wireless Zero Configuration service enabled.
  - Basically, turn it on to let Windows help you abuse wireless.
- My code sucks and I gaurantee there's more efficient ways to do these crazy things.

The Shmoo Group

I didn't know jack about WMI until...

- Google
- http://www.ndis.com/
- “Developing WMI Solutions” by Craig Tunstall and Gwyn Cole
- “Managing Windows with VBScript and WMI” by Don Jones

The Shmoo Group

Summary

- Querying, and in some cases, manipulation of wireless characteristics in Windows is simple with WMI.
- Might not be a replacement for a full-blown commercial WIDS, but consider using WMI.
- Expect wireless to be another OS feature that will be used against you.
- See these examples? Run with 'em!
  - There should be more open source wireless utilities for Windows.

The Shmoo Group

Other Shmoo News

- Airsnort for Windows updated.
  - Much more stable! Thanks Snax!
- Wireless Weaponry live Linux CD SOON.
- ShmooCon! February 4-6, 2005!
  - Marriott Wardman Park in Washington D.C.
  - “Break It!”, “Build It!”, “BoF It!”
  - CFP is out and registration is open
  - $99 until September 30
  - http://www.shmoocon.org
  - Go there to get latest slides and code.

The Shmoo Group

Thanks!

The Shmoo Group