

Hack Your Own Site, or Don't be the Last to Learn the Truth

Dillon Pyron

Principle Security Consultant
NETSerenity, Inc.



Target Audience

- New to security
- Sys admins with security responsibilities

Goals

- Introduce the basics of a vulnerability assessment
- Provide a basic “tool kit” of off-the-shelf open source tools
- Not a how-to-hack

Platforms

- Aimed at both MS and Unix/Linux
- Most tools will run under either environment

2 Tools for Windows

- Cygwin – emulates a Unix environment
 - Has a C/C++ compiler and bash
- Active Perl – a full Perl implementation
- www.cygwin.com
- www.activestate.com
 - Has loads of other tools such as Python & Tcl

Bugtraq

- A solid resource of information on recently discovered bugs and vulnerabilities
- Use it to examine your own network and stay ahead of the game
- Send email to: bugtraq-subscribe@securityfocus.com

Steps to an attack

- Three basic steps to an attack
- Identification
- Vulnerability Assessment
- Vulnerability Exploit
- We'll cover the first two

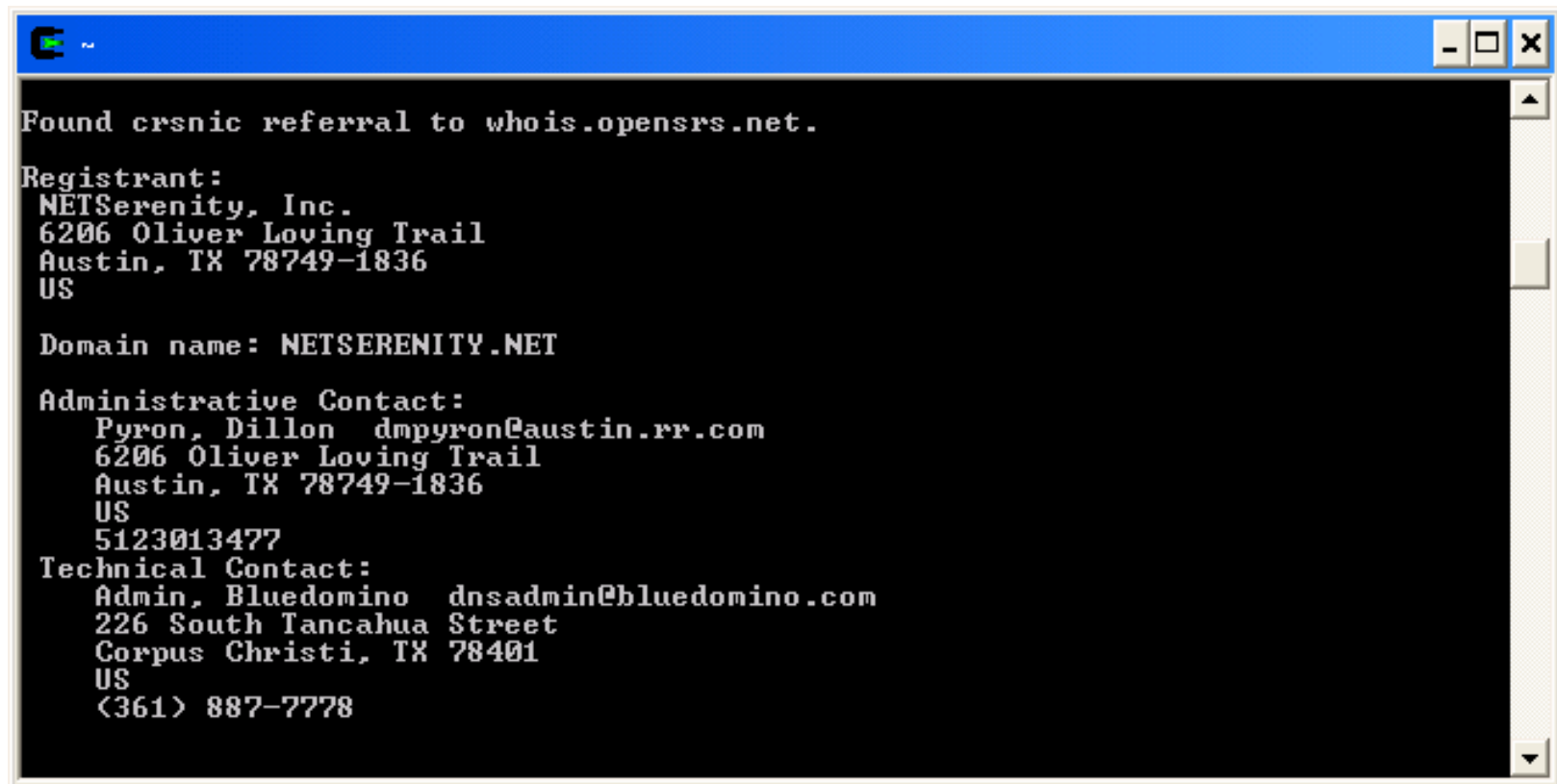
Identification

- Whois
- Nslookup
- Ping
- Traceroute
- Nmap
- Superscan
- Scanline
- LANGuard
- Winfingerprint

Whois

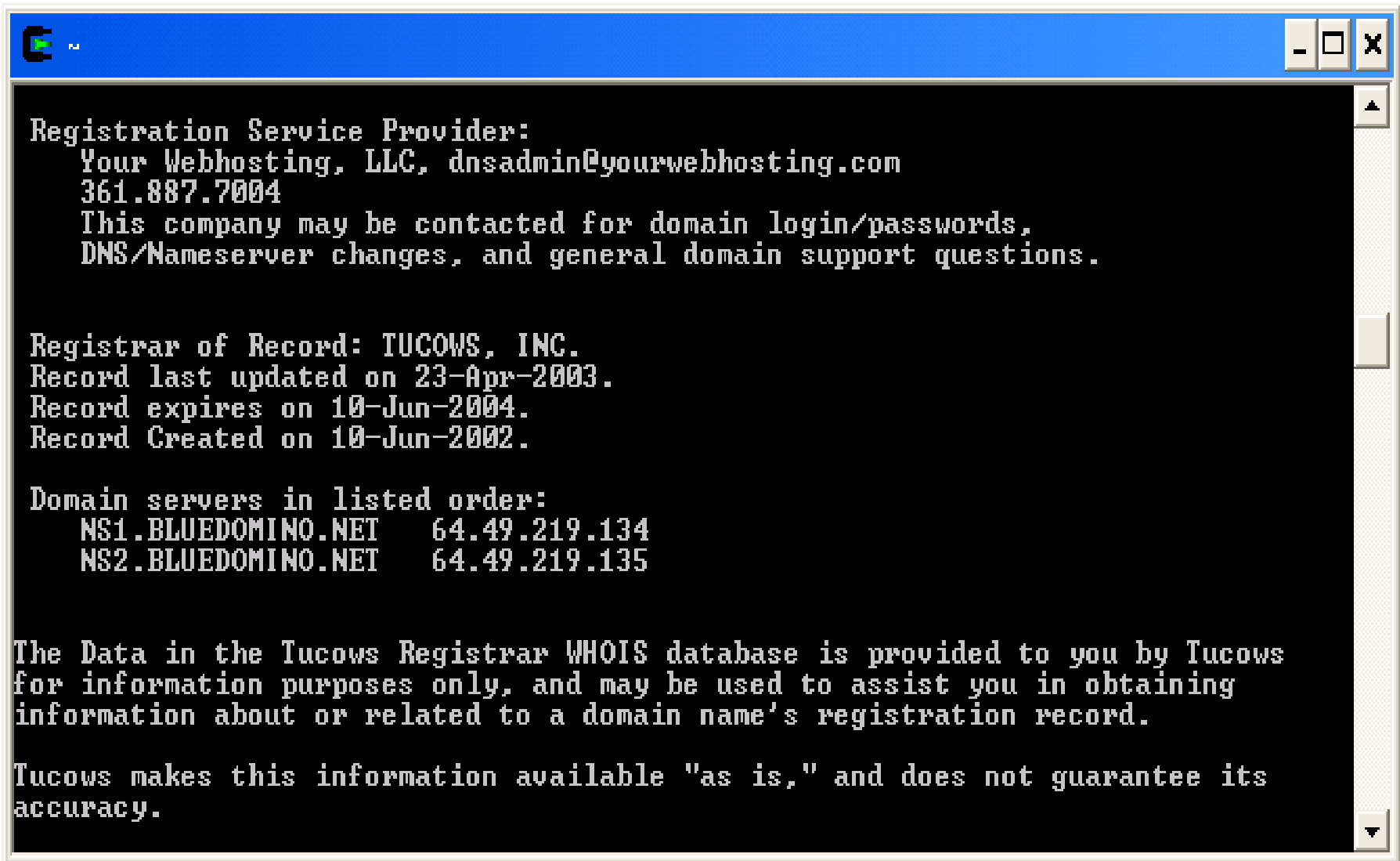
- Standard on Unix/Linux

Whois



```
Found crsnc referral to whois.opensrs.net.  
  
Registrant:  
NETSerenity, Inc.  
6206 Oliver Loving Trail  
Austin, TX 78749-1836  
US  
  
Domain name: NETSERENITY.NET  
  
Administrative Contact:  
Pyron, Dillon dmpyron@austin.rr.com  
6206 Oliver Loving Trail  
Austin, TX 78749-1836  
US  
5123013477  
Technical Contact:  
Admin, Bluedomino dnsadmin@bluedomino.com  
226 South Tanchhua Street  
Corpus Christi, TX 78401  
US  
<361> 887-7778
```

Whois

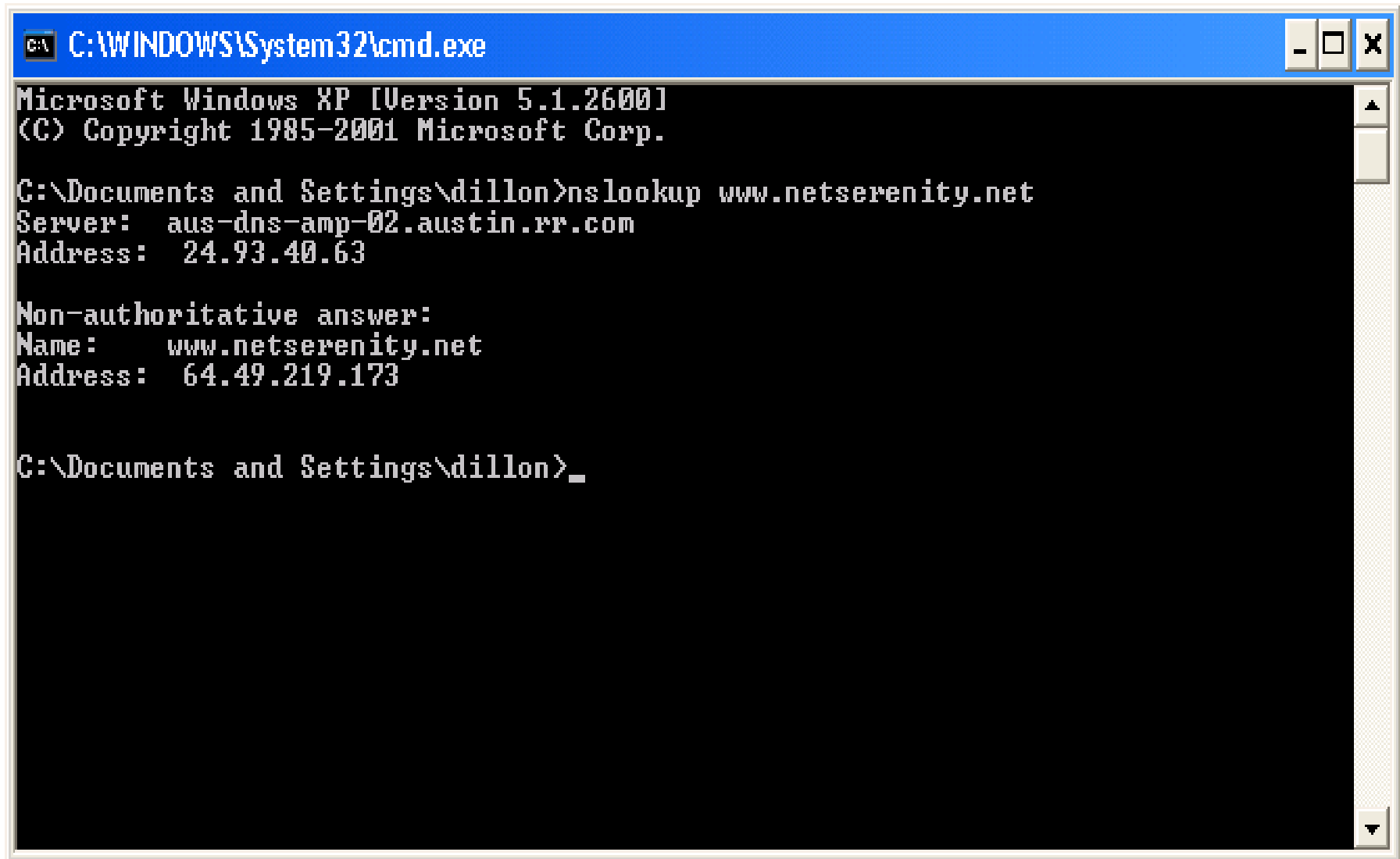


```
Registration Service Provider:  
Your Webhosting, LLC, dnsadmin@yourwebhosting.com  
361.887.7004  
This company may be contacted for domain login/passwords,  
DNS/Nameserver changes, and general domain support questions.  
  
Registrar of Record: TUCOWS, INC.  
Record last updated on 23-Apr-2003.  
Record expires on 10-Jun-2004.  
Record Created on 10-Jun-2002.  
  
Domain servers in listed order:  
NS1.BLUEDOMINO.NET    64.49.219.134  
NS2.BLUEDOMINO.NET    64.49.219.135  
  
The Data in the Tucows Registrar WHOIS database is provided to you by Tucows  
for information purposes only, and may be used to assist you in obtaining  
information about or related to a domain name's registration record.  
  
Tucows makes this information available "as is," and does not guarantee its  
accuracy.
```

Nslookup

- Available on both Unix and Windows

Nslookup



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

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\dillon>nslookup www.netserenity.net
Server:  aus-dns-amp-02.austin.rr.com
Address:  24.93.40.63

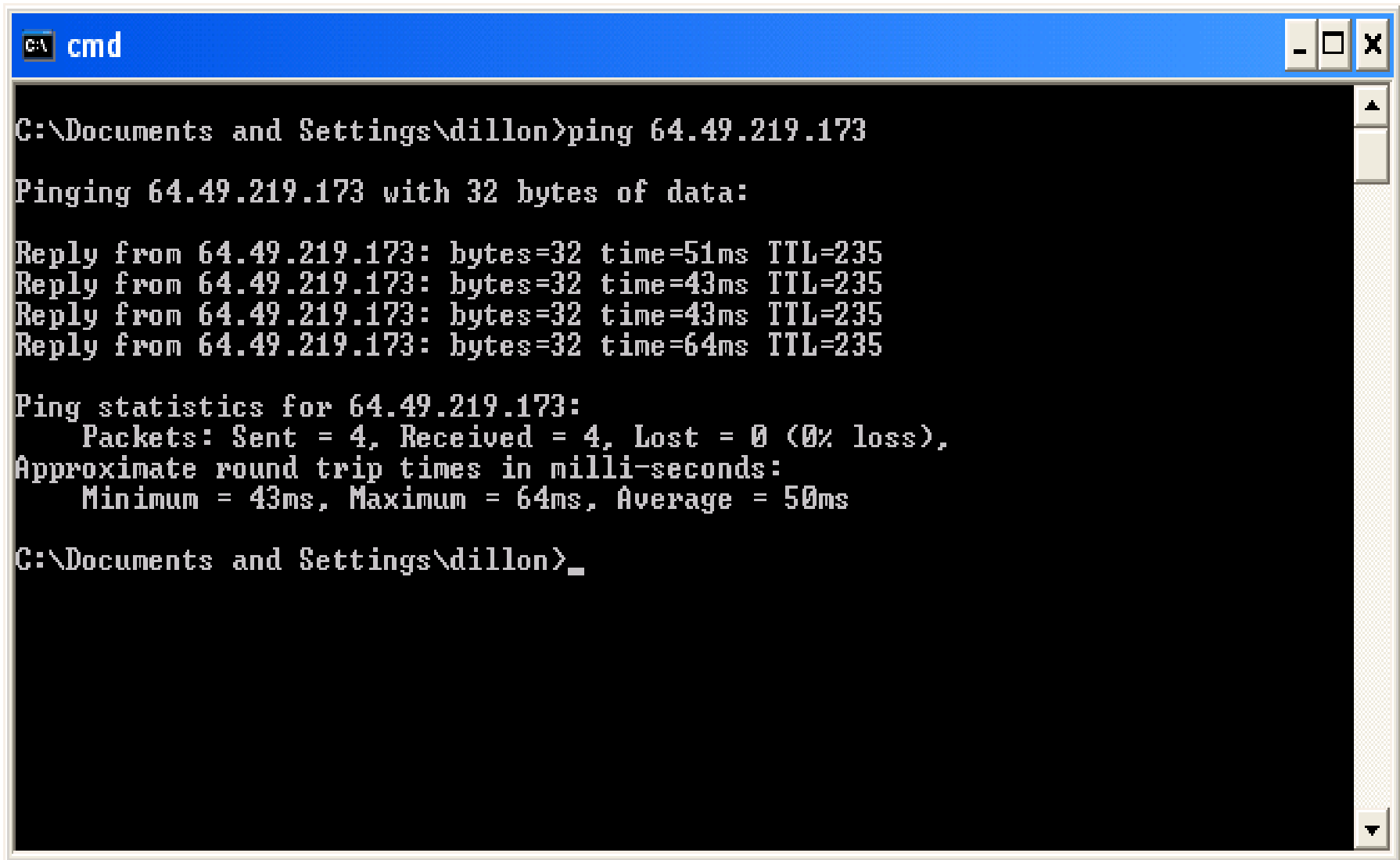
Non-authoritative answer:
Name:     www.netserenity.net
Address:  64.49.219.173

C:\Documents and Settings\dillon>_
```

Ping

- Host “reachable” checking
- Ping works on a single host

Ping



```
C:\Documents and Settings\dillon>ping 64.49.219.173

Pinging 64.49.219.173 with 32 bytes of data:

Reply from 64.49.219.173: bytes=32 time=51ms TTL=235
Reply from 64.49.219.173: bytes=32 time=43ms TTL=235
Reply from 64.49.219.173: bytes=32 time=43ms TTL=235
Reply from 64.49.219.173: bytes=32 time=64ms TTL=235

Ping statistics for 64.49.219.173:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 43ms, Maximum = 64ms, Average = 50ms

C:\Documents and Settings\dillon>_
```

Traceroute

- Provides a path from you to the target
- Can be used to identify potential cut points

Traceroute

```

Tracing route to bluedomino.net [64.49.219.173]
over a maximum of 30 hops:

  0  1    10 ms    23 ms    11 ms    10.34.96.1
    2    12 ms    30 ms     8 ms    pos3-0.austtxs-rtr1.austin.rr.com [66.68.1.37]
    3    11 ms    16 ms    11 ms    srp8-0.austtxrdc-rtr1.austin.rr.com [66.68.1.94]

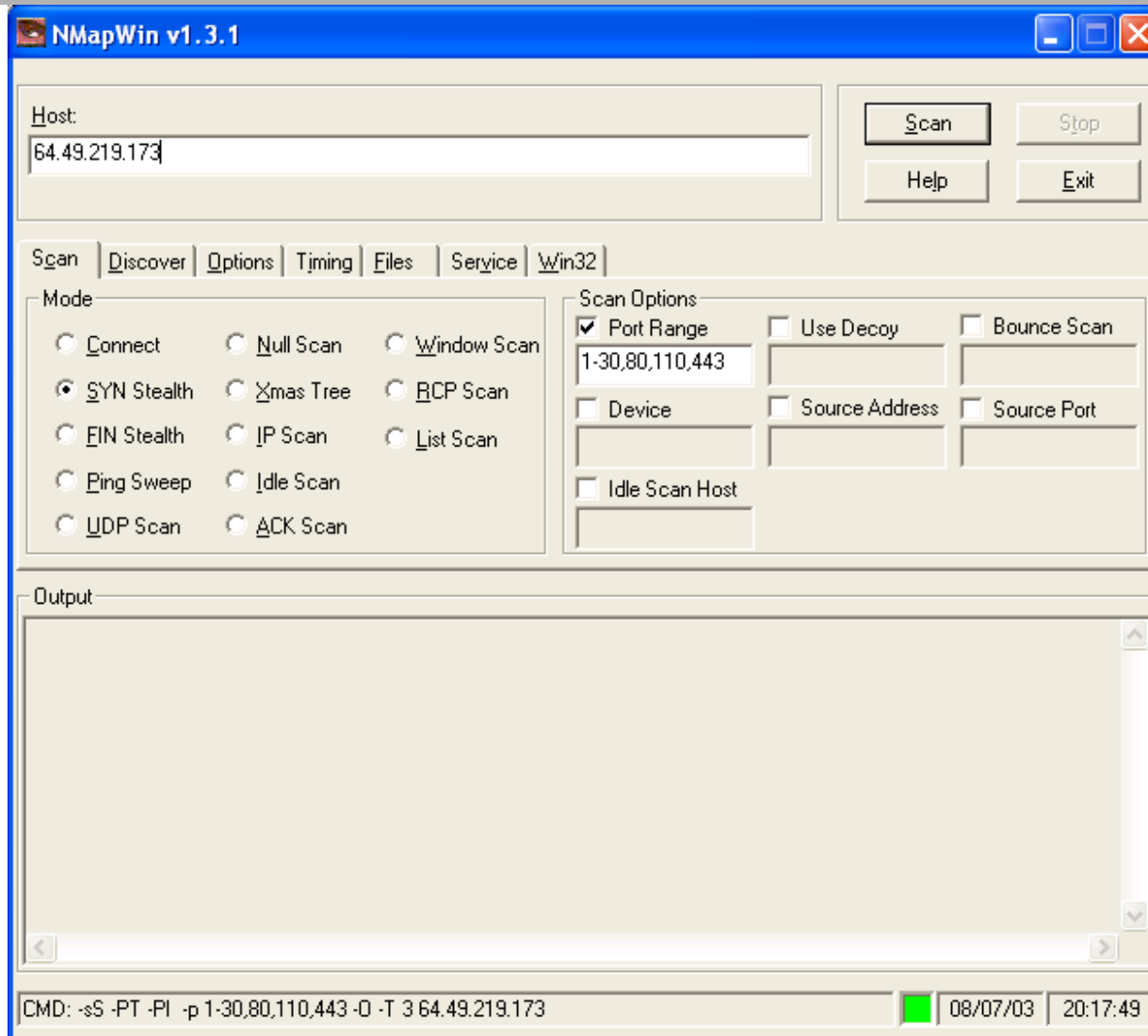
    4    11 ms    15 ms     7 ms    pos1-0.austtxrdc-rtr3.texas.rr.com [66.68.1.102]
    5    12 ms    11 ms    11 ms    pos13-0.austtxrdc-rtr4.texas.rr.com [24.93.33.13]
    6    17 ms    27 ms    15 ms    son0-1-1.hstqtxl3-rtr1.texas.rr.com [24.93.33.22]
    7    17 ms    16 ms    15 ms    pop1-hou-P0-1.atdn.net [66.185.133.145]
    8    33 ms    15 ms    15 ms    bb1-hou-P2-0.atdn.net [66.185.150.148]
    9     *      44 ms    38 ms    bb1-atm-P7-0.atdn.net [66.185.152.184]
   10    36 ms    36 ms    55 ms    pop1-atm-P4-0.atdn.net [66.185.150.1]
   11    36 ms    55 ms    37 ms    sl-bb23-atl-10-2.sprintlink.net [144.232.8.209]

   12    34 ms    34 ms    44 ms    sl-bb25-fw-4-3.sprintlink.net [144.232.20.61]
   13    34 ms     *        63 ms    sl-bb21-fw-12-0.sprintlink.net [144.232.11.25]
   14    36 ms    54 ms     *        sl-gw40-fw-8-0.sprintlink.net [144.232.8.246]
   15    43 ms    44 ms    40 ms    sl-racks-2-0.sprintlink.net [144.232.204.10]
   16    52 ms    45 ms    50 ms    v1130.core1.sat.rackspace.com [64.39.2.33]
   17    43 ms    46 ms    44 ms    v1903.aggr3.sat.rackspace.com [64.39.2.74]
   18    47 ms    43 ms    55 ms    bluedomino.net [64.49.219.173]
  
```

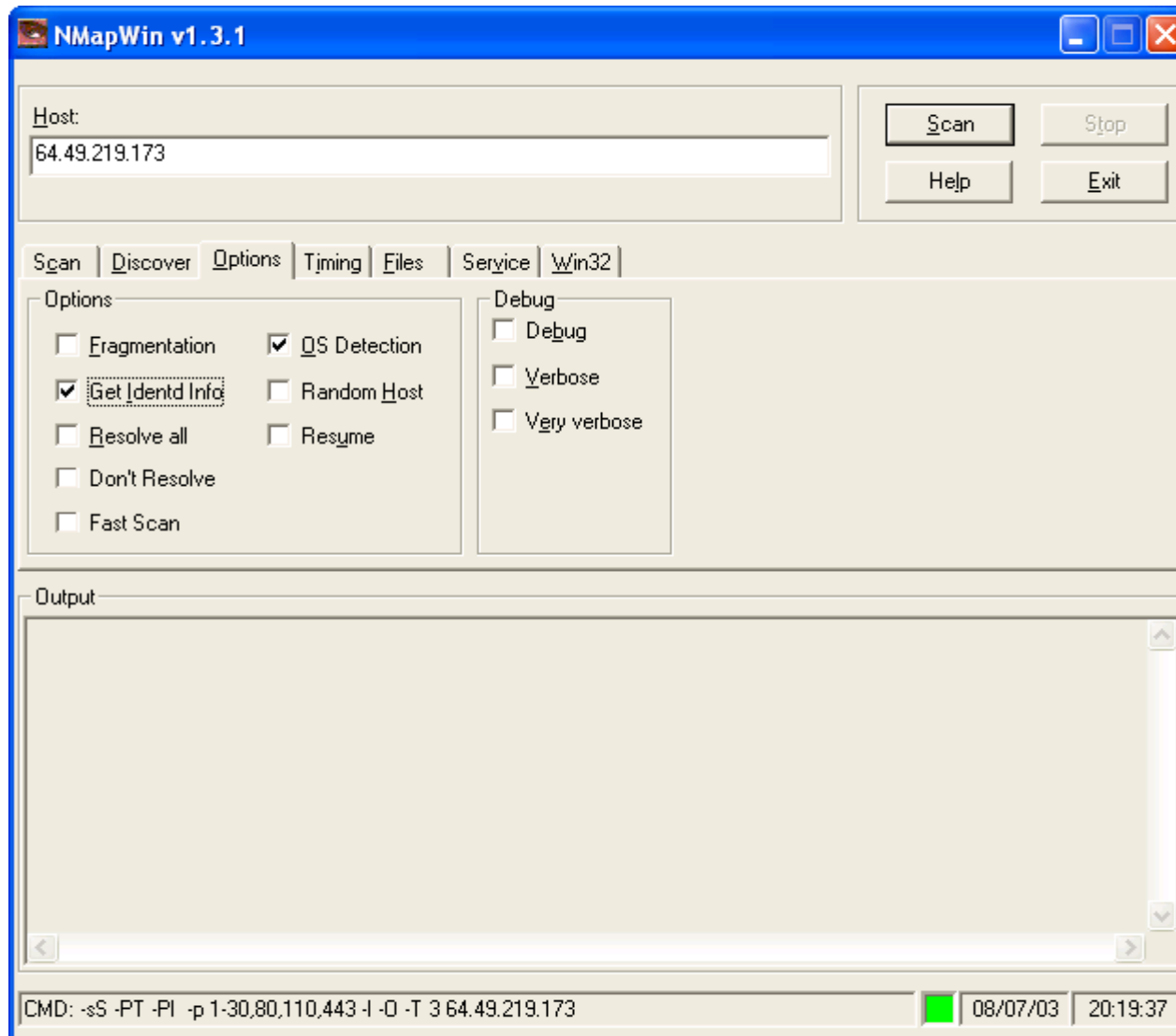
Nmap

- The granddaddy of all port scanners
- Still considered the standard
- Extremely versatile
- www.insecure.org

Nmap



Nmap



Nmap

```

root@pigpen:~
21/tcp      open       ftp
25/tcp      closed    smtp
80/tcp      open       http
110/tcp     open       pop-3
113/tcp     closed    auth

Nmap run completed -- 1 IP address (1 host up) scanned in 167 seconds
[root@pigpen root]# nmap -O 64.49.219.173

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on bluedomino.net (64.49.219.173):
(The 1595 ports scanned but not shown below are in state: filtered)
Port      State      Service
20/tcp    closed    ftp-data
21/tcp    open       ftp
25/tcp    closed    smtp
80/tcp    open       http
110/tcp   open       pop-3
113/tcp   closed    auth
Remote operating system guess: Linux Kernel 2.4.0 - 2.5.20
Uptime 29.156 days (since Fri Jul 11 14:00:26 2003)

Nmap run completed -- 1 IP address (1 host up) scanned in 177 seconds
[root@pigpen root]# █

```

Superscan

- A Windows port scanner

Superscan

SuperScan 3.00

Hostname Lookup
 127.0.0.1
 Resolved

Configuration
 Port list setup

IP
 Start: 64.49.219.173
 Stop: 64.49.219.173
 PrevC NextC 1..254
 Ignore IP zero
 Ignore IP 255
 Extract from file

Timeout
 Ping: 400
 Connect: 2000
 Read: 4000

Scan type
 Resolve hostnames
 Only scan responsive pings
 Show host responses
 Ping only
 Every port in list
 All selected ports in list
 All list ports from 1 65535
 All ports from 1 65535

Scan

Scan Type	Count
Pinging	0
64.49.219.173	0
Scanning	0
64.49.219.173	0
Resolving	0
	0

Start Stop

Speed
 Max
 Min

Active hosts
 1
Open ports
 10

Save
 Collapse all
 Expand all
 Prune

64.49.219.173
 25 Simple Mail Transfer
 21 File Transfer Protocol [Control]
 220 YourWebHosting FTP Server Ready ..
 22 SSH Remote Login Protocol
 SSH-1.99-OpenSSH_2.9p2.
 80 World Wide Web HTTP
 HTTP/1.1 200 OK..Date: Mon, 23 Jun 2003 17:19:07 GMT..Server: A
 110 Post Office Protocol - Version 3
 +OK CPOP3 server ready <web29.bluedomino.net>..
 111 SUN Remote Procedure Call
 514 cmd
 587

Scanline

- Previously known as fscan
- A windows command line port scanner and more
- From FoundStone – www.foundstone.com

Scanline

```

C:\WINDOWS\System32\cmd.exe
D:\Program Files\Tools\scanline>sl -bht 1-30,80,443 64.49.219.173
ScanLine (TM) 1.01
Copyright (c) Foundstone, Inc. 2002
http://www.foundstone.com

Scan of 1 IP started at Mon Jun 23 12:48:10 2003

-----

64.49.219.173
Responded in 60 ms.
20 hops away
Responds with ICMP unreachable: No
TCP ports: 21 22 25 80

TCP 21:
[220 YourWebHosting FTP Server Ready]

TCP 80:
[HTTP/1.1 200 OK Date: Mon, 23 Jun 2003 17:23:48 GMT Server: Apache/1.3.26 (Unix
) mod_gzip/1.3.19.1a Chili!Soft-ASP/3.6.2 mod_throttle/3.1.2 PHP/4.2.2 FrontPal

-----

Scan finished at Mon Jun 23 12:48:14 2003

1 IP and 32 ports scanned in 0 hours 0 mins 4.20 secs

```

LANGuard

- From GFI Software (www.gfi.com)
- Both free and commercial models available
- Commercial model can produce delta reports
- Does some minor vulnerability checking based on services

LANGuard

GFI LANguard Network Scanner v(2.0)

File Edit View Scan Tools LANGuard Help

Target: 64.49.219.173

64.49.219.173 [bluedomino.net] (probably Unix)

- Time to live (TTL) : 235 (255) - 20 hop(s) away
- Open Ports (4)
 - 25 [SmtP => Simple Mail Transfer Protocol]
 - 110 [Pop3 => Post Office Protocol 3]
 - +OK CPOP3 server ready <web29.bluedomino.net>
 - 21 [Ftp => File Transfer Protocol]
 - 220 YourWebHosting FTP Server Ready
 - 80 [Http => World Wide Web, HTTP] Apache/1.3.26 (Unix)
 - HTTP/1.1 400 Bad Request
 - Date: Sun, 13 Jul 2003 02:30:36 GMT
 - Server: Apache/1.3.26 (Unix) mod_gzip/1.3.19.1a Chili!S
 - Connection: close
 - Content-Type: text/html; charset=iso-8859-1

Time to live (TTL) - 235 (255)
+ 20 hop(s) away
- ICMP code in response <> 0 => Unix box
- Timestamp Reply (64.49.219.173)
Ready
1 Computer(s) found.

[64.49.219.173]
Resolving 64.49.219.173...

Port probing (waiting 2 sec) [1/2] ...
bluedomino.net
Port probing (waiting 2 sec) [2/2] ...
4 open port(s).
Gathering banners ...
25 - SMTP
110 - Pop3 => Post Office Protocol 3
21 - FTP
Anonymous logins accepted ?
No
80 - HEAD / HTTP/1.0
Server : Apache/1.3.26 (Unix)
mod_gzip/1.3.19.1a Chili!Soft-ASP/3.6.2
mod_throttle/3.1.2 PHP/4.2.2
FrontPage/5.0.4.3 mod_ssl/2.8.9
OpenSSL/0.9.6c
Operating System : probably Unix
Alerts probing ..
Checking FTP Alerts ...
Checking DNS Alerts ...
Checking Mail Alerts ...
Checking Service Alerts ...
Checking RPC Alerts ...
Checking Miscellaneous ...
Checking Information ...
CGI probing started...
Please wait ...
CGI probing finished.
Ready

Ready

Winfingerprint

- A windows enumeration tool
- Will identify users, shares, services, etc on Windows
- Found at winfingerprint.sourceforge.com

Winfingerprint

Winfingerprint 0.5.8

Input Options

IP Range IP List
 Single Host Neighborhood
 IP Address:

Network Type

NT Domain Active Directory WMI

Scan Options

OS Version Users Registry
 Null Sessions Services NBT Information
 NetBIOS Shares Disks Sessions
 Date and Time Groups Event Log

General Options

Show Error Messages Ping Host(s) TCP Portscan Range: -
 Timeout (in seconds) for TCP/UDP/ICMP/SNMP: RPC Bindings UDP Portscan Range: -
 Retries: Max Connections: SNMP Community String:

Buttons: Scan, Exit, Clear, Save, Help

IP Address: 192.168.1.106 snoopy.austin.rr.com
 NetBIOS: SNOOPY
 Domain: PYRON
 SID: S-1-5-21-971929597-1256799619-874574627
 Pinging 192.168.1.106 with 4 bytes of data:
 Reply from 192.168.1.106: 0 ms (id= 1, seq= 1)
 Reply from 192.168.1.106: 0 ms (id= 2, seq= 2)
 Reply from 192.168.1.106: 0 ms (id= 3, seq= 3)

Fingerprint:

- Role: NT WORKSTATION
- Role: LAN Manager Workstation
- Role: LAN Manager Server
- Role: Server sharing print queue
- Role: Potential Browser
- Role: Master Browser
- Role: Backup Browser
- Version: 5.1
- Comment: snoopy

NetBIOS Shares:

- Name: \\192.168.1.106\E\$ Remark: Default share
- Type: Special share reserved for interprocess communication (IPC\$) or remote administration of the
- Accessible without password.

The “tweeners”

- Not a scanner
- Not a vulnerability assessment tool
- Wotweb – website discovery and identification
- Whisker – CGI analysis
- Shed – Windows share enumeration tool
- Snsnscan – SNMP scanner

Wotweb

- By Robin Keir – keir.net
- A website discovery and identification tool
- Windows GUI display
- Works on individual sites or networks
- Output is “clickable”
- Exports data to Excel spreadsheets

Wotweb

wotweb 1.06 - Robin Keir - keir.net

IPs

Hostname/IP: 64.49.219.173 → Start IP: 64 . 49 . 219 . 173 End IP: 64 . 49 . 219 . 173

Start IP	End IP
24.153.194.1	24.153.194.254
64.49.219.173	

Read IPs from file: Browse...

Web ports to scan

<input checked="" type="checkbox"/> 80	<input type="checkbox"/> 900	<input type="checkbox"/> 3128	<input type="checkbox"/> 7001	<input type="checkbox"/> 8001	<input type="checkbox"/> 8181
<input type="checkbox"/> 81	<input type="checkbox"/> 1214	<input type="checkbox"/> 5000	<input type="checkbox"/> 7002	<input type="checkbox"/> 8010	<input type="checkbox"/> 8888
<input type="checkbox"/> 88	<input type="checkbox"/> 2301	<input type="checkbox"/> 5800	<input type="checkbox"/> 7070	<input checked="" type="checkbox"/> 8080	<input type="checkbox"/> 9090
<input checked="" type="checkbox"/> 443	<input type="checkbox"/> 2779	<input type="checkbox"/> 6588	<input checked="" type="checkbox"/> 8000	<input type="checkbox"/> 8081	<input type="checkbox"/> 10000

Scan Control

Resolve IP addresses
 Randomize scan order
Timeout (ms): 2500

Results Table:

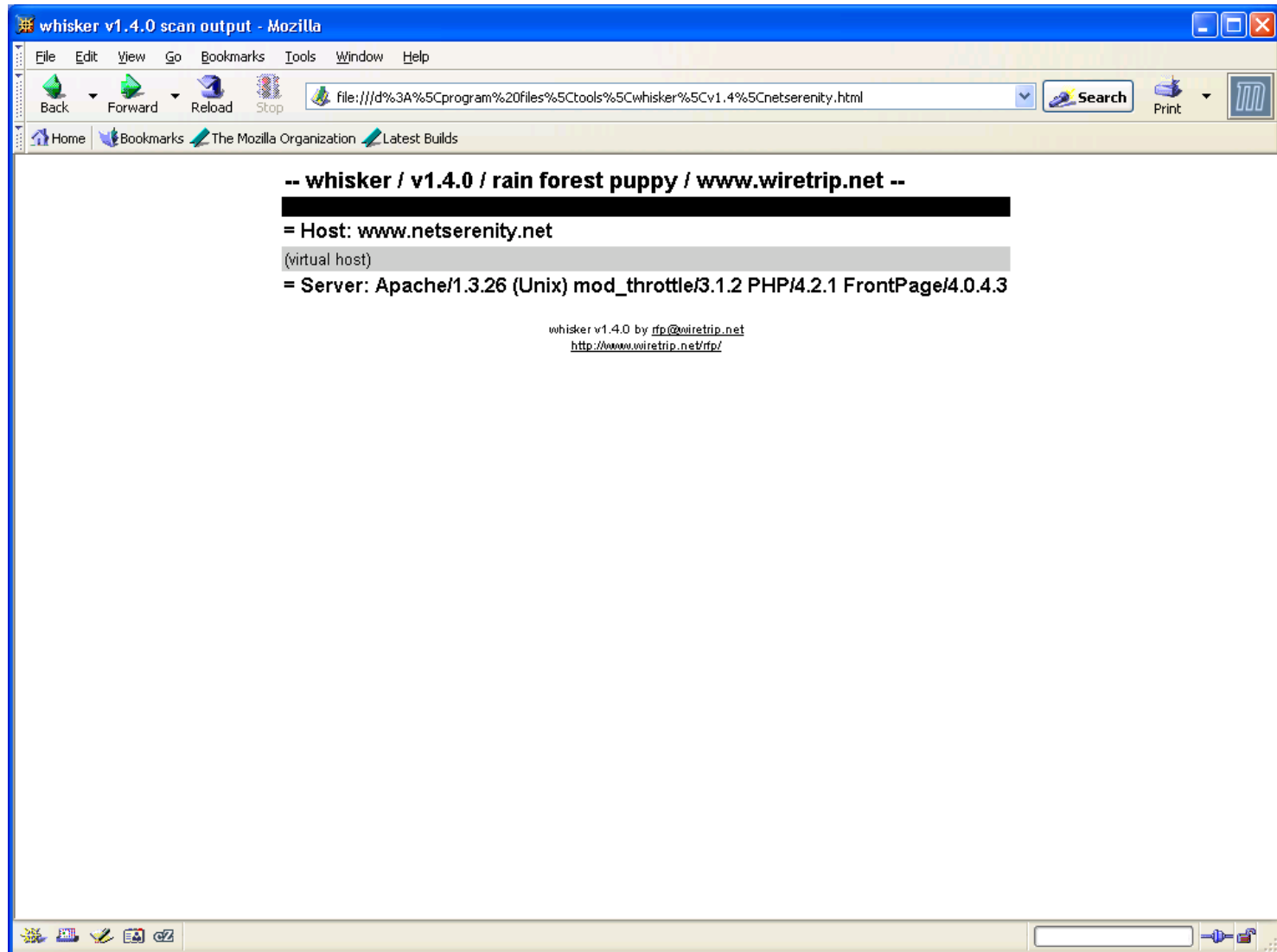
IP	Port	Code	Auth	Server type
24.153.194.17	80	302	None	Apache/1.3.9 (Unix) Red-Hat-Secure/3.1 Apache/Servlet/1.0 mod_s...
24.153.194.100	80	404	None	[Unknown]
24.153.194.10	80	401	Basic	[Unknown]
24.153.194.111	80	401	Basic	ZyXEL-RomPager/3.02
64.49.219.173	80	200	None	Apache/1.3.26 (Unix) mod_gzip/1.3.19.1a Chili!Soft-ASP/3.6.2 mo...
24.153.194.17	443	400	None	Apache/1.3.9 (Unix) Red-Hat-Secure/3.1 Apache/Servlet/1.0 mod_s...
24.153.194.204	8080	401	Basic	[Unknown]
24.153.194.202	8080	401	Basic	[Unknown]

Ports scanned: 1020/1020

Whisker

- A common gateway interface (CGI) scanner
- Found at www.wiretrip.net
- Flexible, extensible, easily updated Perl script

Whisker



Shed

- Used to enumerate shares on Windows systems
- Generates a “clickable” report
- Reports files and devices
- Works on individual systems or networks
- Also from Robin Keir

Shed

The screenshot shows the 'Shed 1.01' application window. The title bar includes the application name, the URL 'http://keir.net', and the local IP address 'This IP: 192.168.1.106'. Below the title bar, there are input fields for 'Start IP' (24.153.194.1) and 'Stop IP' (24.153.194.254), along with a 'Go' button and a 'Hostname Lookup' button. The main area is titled 'Discovered shared resources' and contains a tree view of scan results. The tree shows four IP addresses, each with a list of discovered shares: 24.153.194.64 (IPC\$, SharedDocs), 24.153.194.81 (IPC\$, D\$, ADMIN\$, C\$), 24.153.194.138 (IPC\$), and 24.153.194.211 (C, M, IPC\$). To the right of the tree is an 'Active scans' panel. At the bottom, a summary section shows 'Potential targets' as 7 and 'Shares found' as 4, with a 'Finished' button, 'Options' button, and 'About' button.

Shed 1.01 http://keir.net This IP: 192.168.1.106

Start IP 24 . 153 . 194 . 1

Stop IP 24 . 153 . 194 . 254

Go

Hostname Lookup

Discovered shared resources Collapse Expand Active scans

- 24.153.194.64 - rrcs-sw-24-153-194-64.biz.rr.com
 - IPC\$ [Remote IPC]
 - SharedDocs
- 24.153.194.81 - rrcs-sw-24-153-194-81.biz.rr.com
 - IPC\$ [Remote IPC]
 - D\$ [Default share]
 - ADMIN\$ [Remote Admin]
 - C\$ [Default share]
- 24.153.194.138 - rrcs-sw-24-153-194-138.biz.rr.com
 - IPC\$ [Remote IPC]
- 24.153.194.211 - rrcs-sw-24-153-194-211.biz.rr.com
 - C
 - M
 - IPC\$ [Remote Inter Process Communication]

Potential targets 7

Shares found 4

Finished Options About

Snscan

- A simple SNMP scanner
- You provide the community name, it locates the service
- Developed in response to the SNMP vulnerabilities discovered in late 2001
- Another Foundstone tool

Snscan

SNScan 1.04 -- Copyright © Foundstone Inc. -- http://www.foundstone.com

IP addresses to scan

Hostname/IP: ->

Start IP: ->

End IP: ->

Read IPs from file:

Start IP	End IP
192.168.1.1	192.168.1.254
64.49.219.173	

SNMP ports to scan

161 391
 193 1993

SNMP community string

Scan control

Randomize scan order

Timeout (ms):

IP	Port	Description
192.168.1.100	161	-- Unknown --

Ports scanned: 255/255

Vulnerability Scanners

- Powerful tools
- Scanners enumerate vulnerabilities
- They look for known bugs and misconfigured software

Nessus

- Found at www.nessus.org
- A remote scanner
- Operates in a client/server relationship
- Server is Unix/Linux
- Clients available for Unix, Linux and most Windows

Nessus

- Uses nmap and GTK
- Modular design permits easy updates of database
- Easy to use GUI front-end
- Updates provided by nessus.org and can be easily scripted
- Output in text, HTML and LaTeX

Internet Scanner

- Check www.iss.net for details
- Commercial product
- A remote scanner
- Standalone
- Windows only, but will scan Unix

Internet Scanner

- Has a remote update feature for database
- Vulnerabilities can be scripted
- GUI
- Output in HTML and PDF
- Produces “executive” level graphs

Miscellaneous

- Wireless scanners
 - Netstumbler
 - AiropEEK
- Wardialers
 - Tone-Loc

Miscellaneous

- Sniffers
 - Ethereal
 - Tcpdump
 - Dsniff
- Password crackers
 - John the Ripper

Wireless scanners

- Both give the ability to detect and identify WLANs
- AiroPeek also has a packet capture facility, if you have the WEP key (or they're not WEPed)

Netstumbler

Network Stumbler - [LA Convention Center 24-SEP-2002]

File Edit View Options Window Help

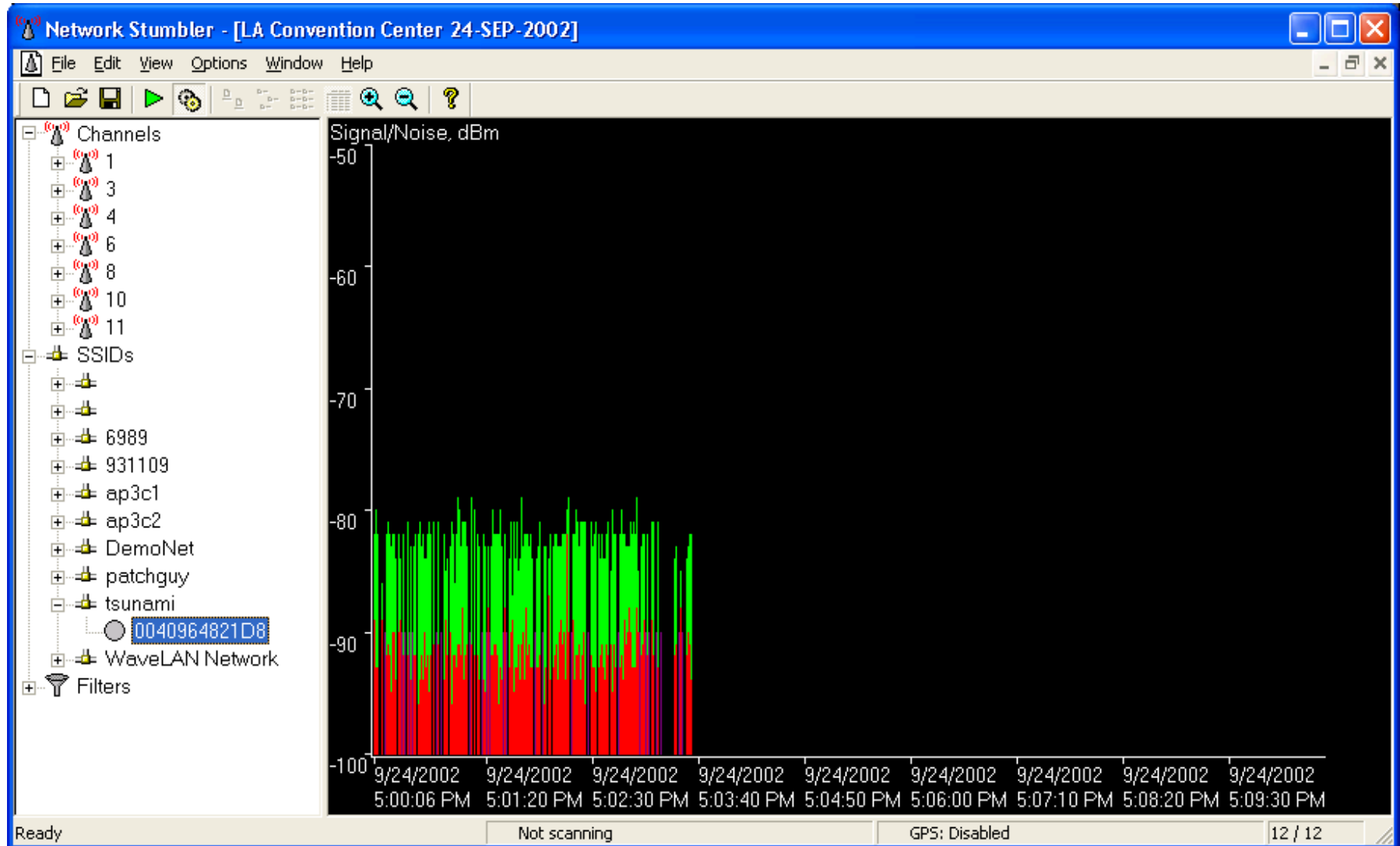
Channels

- 1
- 3
- 4
- 6
- 8
- 10
- 11
- SSIDs
- Filters

MAC	SSID	Name	Ch...	Vendor	Ty...	W...	SN...	Sign...	Noi...	SN..
0002B3A5D2B8	6989		11	Intel	AP			-86	-94	8
0060B3709C55	patchguy		1	Z-Com	AP			-85	-91	6
00508B9921A2	DemoNet		6	Comp...	AP			-85	-95	8
00022D32DC88	ap3c1		3	Agere...	AP			-80	-94	11
005018065F84	931109		8	Advan...	AP			-84	-95	11
00022D15A6F2		AP-1000_0...		Agere...				0	0	0
00022D19FC74		AP-1000_0...		Agere...				0	0	0
00022D27F8B9			10	Agere...	AP			-80	-93	13
00022D32DD84	ap3c2		4	Agere...	AP			-79	-93	14
0040964821D8	tsunami		3	Cisco ...	AP			-79	-96	15
00022D32DCC8	WaveLAN Network	AP-1000_0...	10	Agere...	AP			-67	-93	24
00022D2E5FDE	WaveLAN Network	AP-1000_0...	10	Agere...	AP			-67	-93	25

Ready Not scanning GPS: Disabled 12 / 12

Netstumbler



AiroPeek

AiroPeek Demo - [HTTP-UnWEP.apc]

File Edit View Capture Statistics Tools Window Help

Packets: 250

Packet	Source	Destination	BSSID	Data Rate	Channel	Signal	Flags	Size	Absolute Time	Protocol
224		00:A0:F8:9B:B9:AA		1.0	11	81%	#	14	13:04:42.624368	802.11 A
225	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	11	81%	*	71	13:04:42.630577	802.11 B
226	IP-192.216.124.4	IP-192.168.0.11	00:A0:F8:8B:20:1F	11.0	11	81%		326	13:04:42.726398	TCP HTTP
227		00:A0:F8:8B:20:1F		1.0	11	48%	#	14	13:04:42.726497	802.11 A
228	IP-192.168.0.11	IP-192.216.124.4	00:A0:F8:8B:20:1F	11.0	11	45%		447	13:04:42.729439	TCP HTTP
229		00:A0:F8:9B:B9:AA		1.0	11	61%	#	14	13:04:42.729533	802.11 A
230	IP-192.216.124.4	IP-192.168.0.11	00:A0:F8:8B:20:1F	11.0	11	61%		326	13:04:42.730586	TCP HTTP
231		00:A0:F8:8B:20:1F		1.0	11	45%	#	14	13:04:42.730680	802.11 A
232	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	11	61%	*	71	13:04:42.733115	802.11 B
233	IP-192.168.0.11	IP-192.216.124.4	00:A0:F8:8B:20:1F	11.0	11	90%		448	13:04:42.734111	TCP HTTP
234		00:A0:F8:9B:B9:AA		1.0	11	61%	#	14	13:04:42.734204	802.11 A
235	IP-192.216.124.4	IP-192.168.0.11	00:A0:F8:8B:20:1F	11.0	11	45%		326	13:04:42.834759	TCP HTTP
236		00:A0:F8:8B:20:1F		1.0	11	48%	#	14	13:04:42.834859	802.11 A
237	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	11	84%	*	71	13:04:42.836580	802.11 B
238	IP-192.168.0.11	IP-192.216.124.4	00:A0:F8:8B:20:1F	11.0	11	90%		450	13:04:42.837616	TCP HTTP
239		00:A0:F8:9B:B9:AA		1.0	11	45%	#	14	13:04:42.837710	802.11 A
240	IP-192.216.124.4	IP-192.168.0.11	00:A0:F8:8B:20:1F	11.0	11	52%		326	13:04:42.839603	TCP HTTP
241		00:A0:F8:8B:20:1F		1.0	11	87%	#	14	13:04:42.839697	802.11 A
242	IP-192.168.0.11	IP-192.216.124.4	00:A0:F8:8B:20:1F	11.0	11	90%		444	13:04:42.842326	TCP HTTP
243		00:A0:F8:9B:B9:AA		1.0	11	84%	#	14	13:04:42.842421	802.11 A
244	00:A0:F8:8B:20:1F	Broadcast	00:A0:F8:8B:20:1F	1.0	11	87%	*	71	13:04:42.937739	802.11 B
245	IP-192.216.124.4	IP-192.168.0.11	00:A0:F8:8B:20:1F	11.0	11	87%		326	13:04:42.947522	TCP HTTP
246		00:A0:F8:8B:20:1F		1.0	11	52%	#	14	13:04:42.947623	802.11 A
247	IP-192.168.0.11	IP-192.216.124.4	00:A0:F8:8B:20:1F	11.0	11	55%		446	13:04:42.950270	TCP HTTP
248		00:A0:F8:9B:B9:AA		1.0	11	84%	#	14	13:04:42.950368	802.11 A
249	IP-192.216.124.4	IP-192.168.0.11	00:A0:F8:8B:20:1F	11.0	11	84%		325	13:04:42.951774	TCP HTTP
250		00:A0:F8:8B:20:1F		1.0	11	52%	#	14	13:04:42.951869	802.11 A

Packets Nodes Protocols Conversations Size Summary History Log

Network Statistics

Gauge Value

Messages: 3

Date	Time	Message
07/06/2003	21:20:21	AiroPeek Demo started
07/06/2003	21:22:28	AiroPeek Demo quit
07/07/2003	23:34:56	AiroPeek Demo started

For Help, press F1

AiroPeek

AiroPeek Demo - [HTTP-UnWEP.apc]

File Edit View Capture Statistics Tools Window Help

Packets: 250

BSSID	Data Rate	Channel	Signal	Flags	Size	Absolute Time	Protocol	Summary
	1.0	11	81%	#	14	13:04:42.624368	802.11 Ack	FC=.....
00:A0:F8:8B:20:1F	1.0	11	81%	*	71	13:04:42.630577	802.11 Beacon	FC=.....,SN=1669,FN= 0,BI=100...
00:A0:F8:8B:20:1F	11.0	11	81%		326	13:04:42.726398	TCP HTTP	.AP...,S=3216490909,L= 250,A=33...
	1.0	11	48%	#	14	13:04:42.726497	802.11 Ack	FC=.....
00:A0:F8:8B:20:1F	11.0	11	45%		447	13:04:42.729439	TCP HTTP	/images/hm/hm_contact_over.gif
	1.0	11	61%	#	14	13:04:42.729533	802.11 Ack	FC=.....
00:A0:F8:8B:20:1F	11.0	11	61%		326	13:04:42.730586	TCP HTTP	.AP...,S=1048799909,L= 250,A=33...
	1.0	11	45%	#	14	13:04:42.730680	802.11 Ack	FC=.....
00:A0:F8:8B:20:1F	1.0	11	61%	*	71	13:04:42.733115	802.11 Beacon	FC=.....,SN=1672,FN= 0,BI=100...
00:A0:F8:8B:20:1F	11.0	11	90%		448	13:04:42.734111	TCP HTTP	/images/hm/hm_partners_over.gif
	1.0	11	61%	#	14	13:04:42.734204	802.11 Ack	FC=.....
00:A0:F8:8B:20:1F	11.0	11	45%		326	13:04:42.834759	TCP HTTP	.AP...,S=3216491159,L= 250,A=33...
	1.0	11	48%	#	14	13:04:42.834859	802.11 Ack	FC=.....
00:A0:F8:8B:20:1F	1.0	11	84%	*	71	13:04:42.836580	802.11 Beacon	FC=.....,SN=1674,FN= 0,BI=100...
00:A0:F8:8B:20:1F	11.0	11	90%		450	13:04:42.837616	TCP HTTP	/images/hm/hm_employment_over.gif
	1.0	11	45%	#	14	13:04:42.837710	802.11 Ack	FC=.....
00:A0:F8:8B:20:1F	11.0	11	52%		326	13:04:42.839603	TCP HTTP	.AP...,S=1048800159,L= 250,A=33...
	1.0	11	87%	#	14	13:04:42.839697	802.11 Ack	FC=.....
00:A0:F8:8B:20:1F	11.0	11	90%		444	13:04:42.842326	TCP HTTP	/images/hm/hm_sales_over.gif
	1.0	11	84%	#	14	13:04:42.842421	802.11 Ack	FC=.....
00:A0:F8:8B:20:1F	1.0	11	87%	*	71	13:04:42.937739	802.11 Beacon	FC=.....,SN=1676,FN= 0,BI=100...
00:A0:F8:8B:20:1F	11.0	11	87%		326	13:04:42.947522	TCP HTTP	.AP...,S=3216491409,L= 250,A=33...
	1.0	11	52%	#	14	13:04:42.947623	802.11 Ack	FC=.....
00:A0:F8:8B:20:1F	11.0	11	55%		446	13:04:42.950270	TCP HTTP	/images/hm/hm_digits_over.gif
	1.0	11	84%	#	14	13:04:42.950368	802.11 Ack	FC=.....
00:A0:F8:8B:20:1F	11.0	11	84%		325	13:04:42.951774	TCP HTTP	.AP...,S=1048800409,L= 249,A=33...
	1.0	11	52%	#	14	13:04:42.951869	802.11 Ack	FC=.....

Packets Nodes Protocols Conversations Size Summary History Log

Network Statistics

Gauge Value

Messages: 3

Date	Time	Message
07/06/2003	21:20:21	AiroPeek Demo started
07/06/2003	21:22:28	AiroPeek Demo quit
07/07/2003	23:34:56	AiroPeek Demo started

AiroPeek Demo Log

For Help, press F1

Wardialers

- Allows automated dialing and identification
- Locates modems, fax machines and line redirects

Sniffers

- Pull in and (optionally) parse raw packets
- WinDump is a Windows implementation of tcpdump
- Ethereal breaks down packets for easier analysis
- Dsniff is a collection of tools, some very powerful and dangerous

Ethereal

<capture> - Ethereal

File Edit Capture Display Tools Help

No.	Time	Source	Destination	Protocol	Info
397	48.015319	Sony_58:c2:e0	01:80:c2:00:00:00	STP	Conf. Root = 32768/b2:5c:08:8e:d2:2d Cost = 0 Port = 0x
401	50.016029	Sony_58:c2:e0	01:80:c2:00:00:00	STP	Conf. Root = 32768/b2:5c:08:8e:d2:2d Cost = 0 Port = 0x
408	52.016583	Sony_58:c2:e0	01:80:c2:00:00:00	STP	Conf. Root = 32768/b2:5c:08:8e:d2:2d Cost = 0 Port = 0x
412	54.017227	Sony_58:c2:e0	01:80:c2:00:00:00	STP	Conf. Root = 32768/b2:5c:08:8e:d2:2d Cost = 0 Port = 0x
414	56.017861	Sony_58:c2:e0	01:80:c2:00:00:00	STP	Conf. Root = 32768/b2:5c:08:8e:d2:2d Cost = 0 Port = 0x
13	9.345176	212.100.234.54	pigpen	HTTP	Continuation
15	9.471421	212.100.234.54	pigpen	HTTP	Continuation
17	9.472685	212.100.234.54	pigpen	HTTP	Continuation
18	9.478982	212.100.234.54	pigpen	HTTP	Continuation
21	9.598232	212.100.234.54	pigpen	HTTP	Continuation
23	9.599519	212.100.234.54	pigpen	HTTP	Continuation
24	9.603689	212.100.234.54	pigpen	HTTP	Continuation
26	9.610217	212.100.234.54	pigpen	HTTP	Continuation
27	9.617596	212.100.234.54	pigpen	HTTP	Continuation
33	9.724071	212.100.234.54	pigpen	HTTP	Continuation
34	9.725748	212.100.234.54	pigpen	HTTP	Continuation

Frame 15 (1434 on wire, 1434 captured)

- Ethernet II
- Internet Protocol, Src Addr: 212.100.234.54 (212.100.234.54), Dst Addr: pigpen (192.168.1.105)
 - Version: 4
 - Header length: 20 bytes
 - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 - Total Length: 1420
 - Identification: 0x8aa2
 - Flags: 0x04
 - Fragment offset: 0
 - Time to live: 47
 - Protocol: TCP (0x06)
 - Header checksum: 0x3b1d (correct)
 - source: 212.100.234.54 (212.100.234.54)
 - destination: pigpen (192.168.1.105)
- Transmission Control Protocol, Src Port: http (80), Dst Port: 1082 (1082), Seq: 1253607842, Ack: 1876331482, Len: 1380
 - source port: http (80)
 - destination port: 1082 (1082)
 - Sequence number: 1253607842
 - Next sequence number: 1253609222

```

0000  00 07 95 f2 f7 b2 00 04 5a ef 5f df 08 00 45 00  .....Z.....E.
0010  05 8c 8a a2 40 00 2f 06 3b 1d d4 64 ea 36 c0 a8  ....@./.;..d.6..
0020  01 69 00 50 04 3a 4a b8 89 a2 6f d6 8b da 50 10  .i.P.:J. .o...P.
0030  19 20 10 98 00 00 3c 74 72 3e 3c 74 64 20 61 6c  . . . .<t r><td a\
0040  69 67 6e 3d 22 63 65 6e 74 65 72 22 3e 3c 74 61  ign="cen ter"><ta
  
```

Filter: Reset Apply File: <capture> Drops: 0

Password Crackers

- John the Ripper cracks multiple password formats
- Can crack one OS's passwords on another platform
- Found at www.openwall.com/john
- Can be set up to do distributed cracking
- Speed varies with the encryption algorithm
- Can use various “dictionaries” to increase effectiveness

John the Ripper

```
cmd
D:\Program Files\Tools\John\john-16\run>john -test
Benchmarking: Standard DES [24/32 4K]... DONE
Many salts:      140335 c/s
Only one salt:   136144 c/s

Benchmarking: BSDI DES (x725) [24/32 4K]... DONE
Many salts:      4927 c/s
Only one salt:   4956 c/s

Benchmarking: FreeBSD MD5 [32/32]... DONE
Raw:             3305 c/s

Benchmarking: OpenBSD Blowfish (x32) [32/32]... DONE
Raw:             196 c/s

Benchmarking: Kerberos AFS DES [24/32 4K]... DONE
Short:           129887 c/s
Long:            328204 c/s

Benchmarking: NT LM DES [24/32 4K]... DONE
Raw:             444760 c/s

D:\Program Files\Tools\John\john-16\run>
```

Putting it all together

- Nessus is the premier open source tool
- For Unix get nmap and whisker
- For Windows get Internet Scanner, shed, wotweb and whisker
- Schedule periodic scans and keep all tools up-to-date
- Do SOMETHING!

Questions?



HP WORLD 2003

Solutions and Technology Conference & Expo

Interex, Encompass and HP bring you a powerful new HP World.

