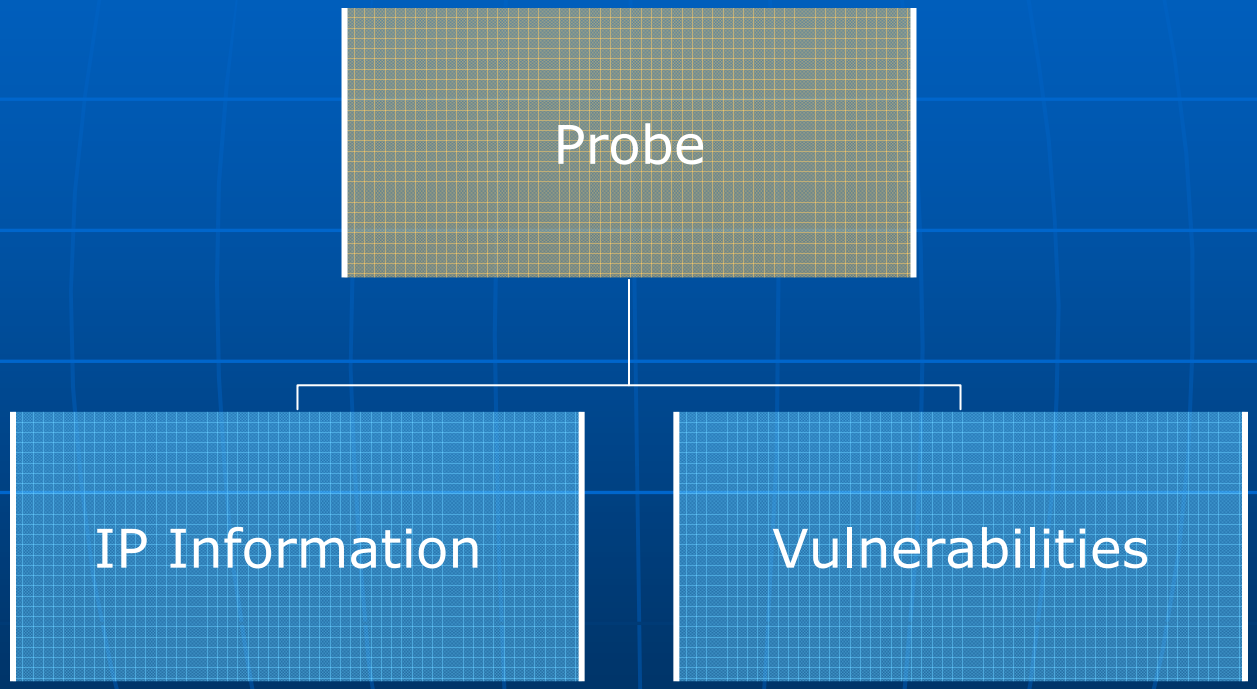
Identification of Pakistan's IP Information & Vulnerability Assessment

Nizar Diamond Ali

PakCon, Karachi
Dec 2004

Aim



Aim (Cont…)

- Detailed IP information of Pakistan was not available as a directory prior to this study
- May be not to general public
- It's generally not known how to harvest this information
  - Through websites?
  - Asking?
  - Using tools?

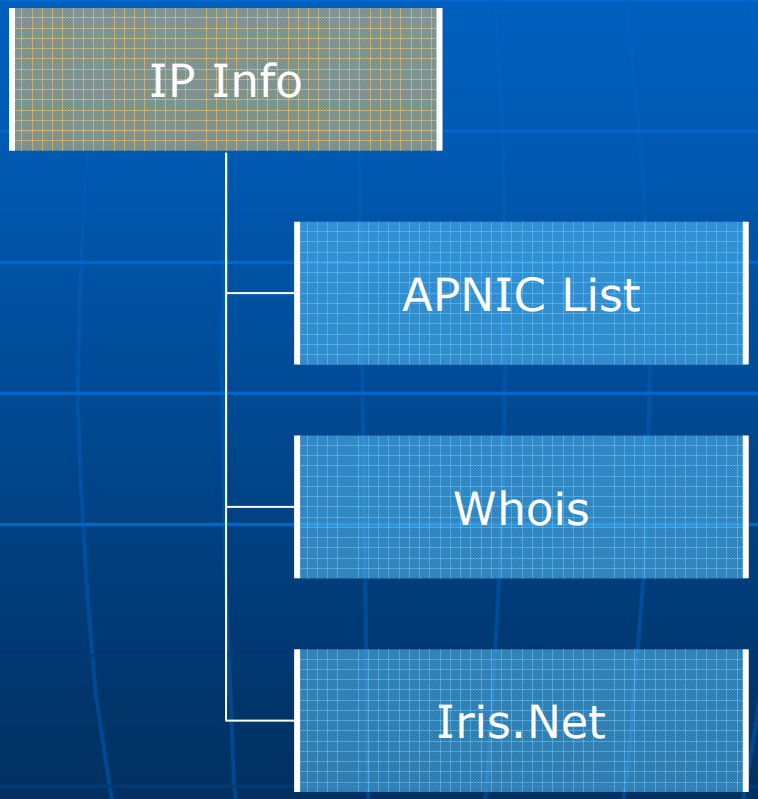
Aim (Cont…)

- This information leads to subtle clues about state of networks in our country. Assigned IP blocks listing serves as a directory to lookup an IP and tell exactly if it belongs to a Pakistani network service provider.
- The other detail gathered provides vital information about network's devices (for example router's operating systems) and names and version of web servers in use.
- This information combined with vulnerability assessment data is more than enough to show where networks of Pakistan can be attempted for exploitations.

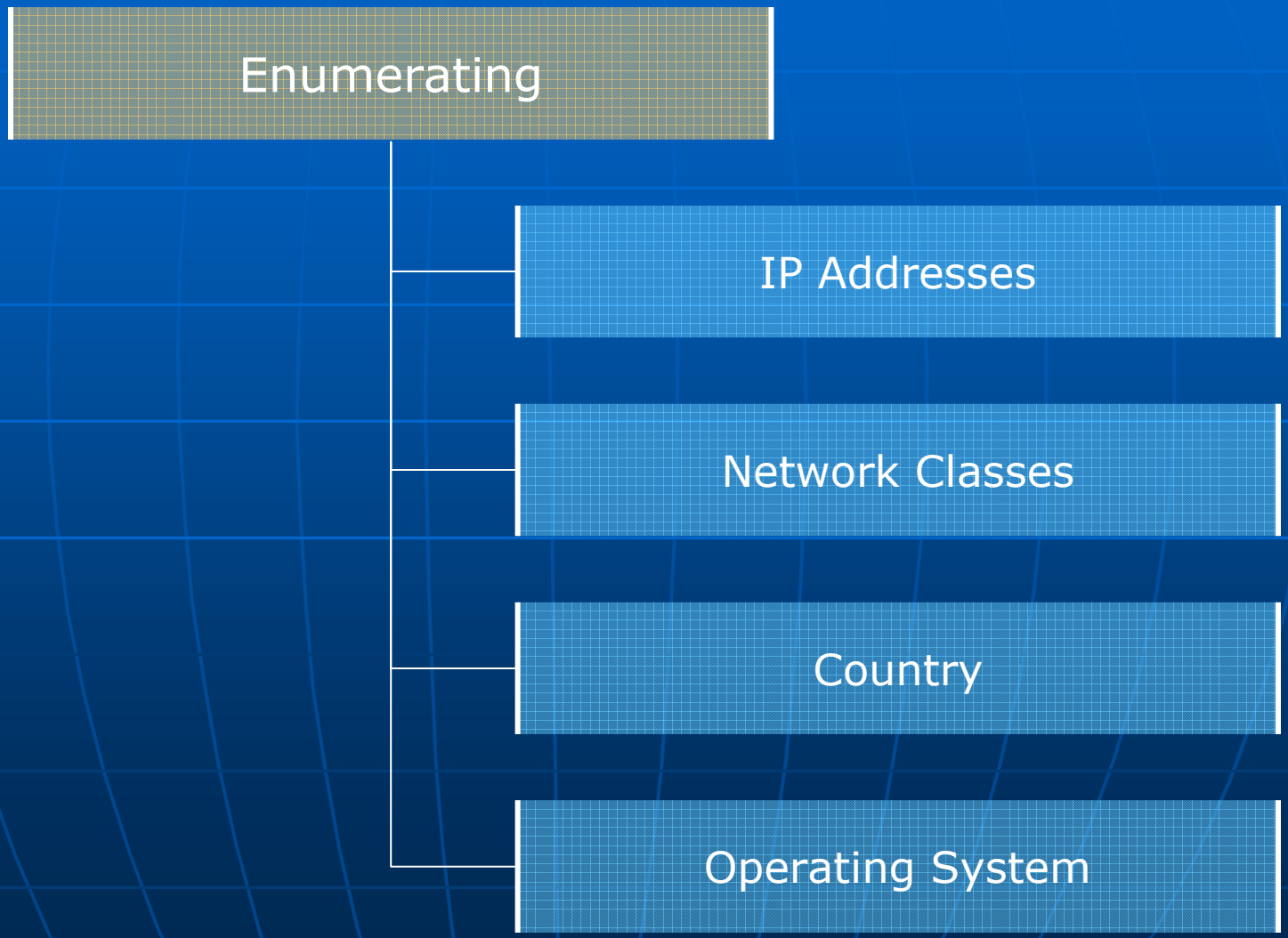
What Was Enumerated?

- IP ranges assigned to Pakistan
- Network Service Providers (NSPs) operating in Pakistan
- Detailed information (ex: services, vulnerabilities) on NSPs w/o contacting them –using only available to all and free means

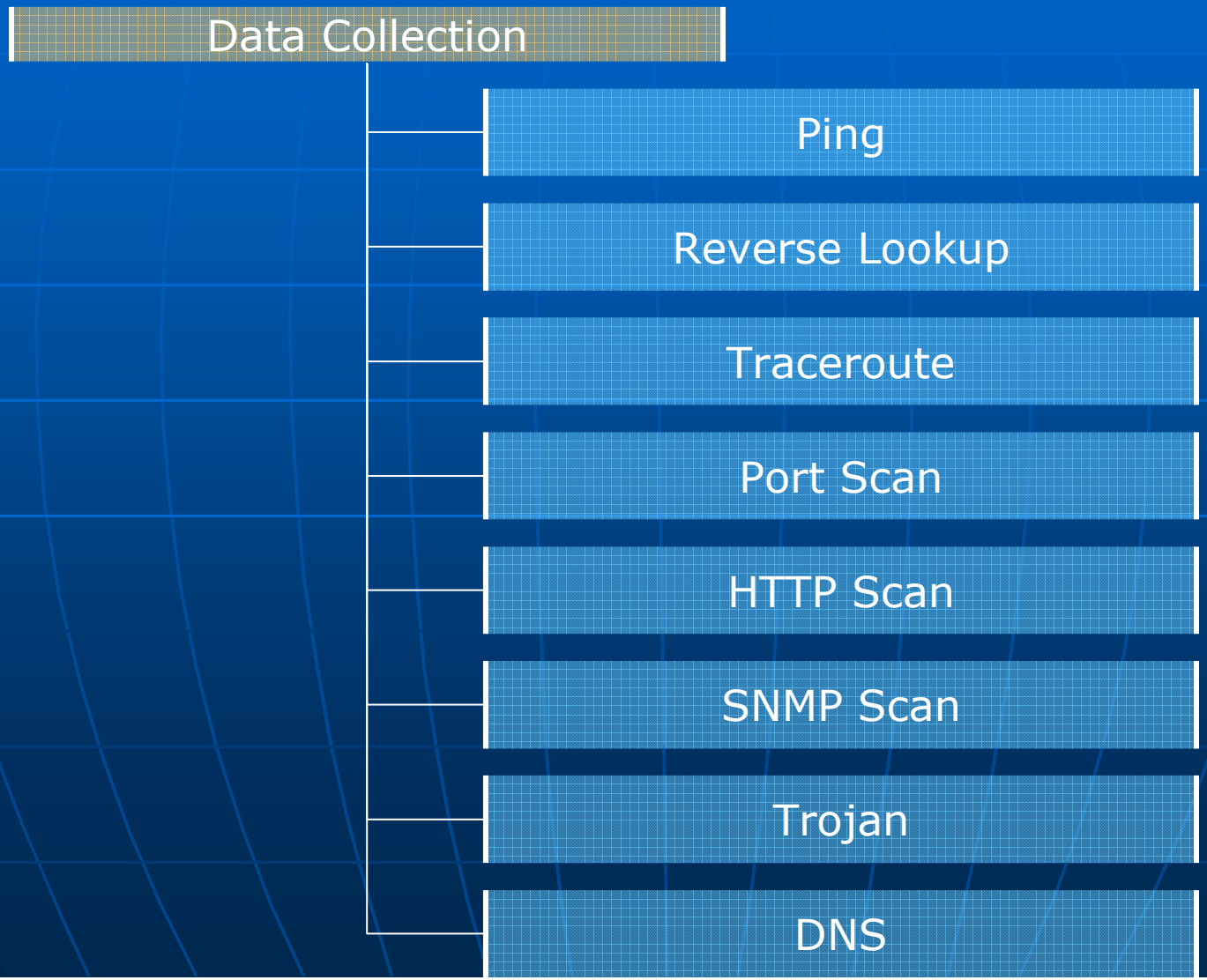
Operations Performed



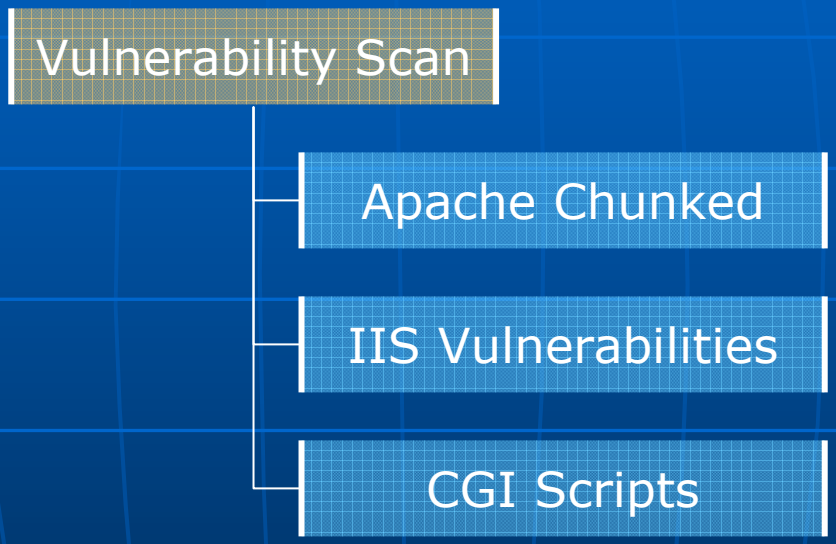
Operations Performed (Cont…)



Operations Performed (Cont…)



Operations Performed (Cont…)

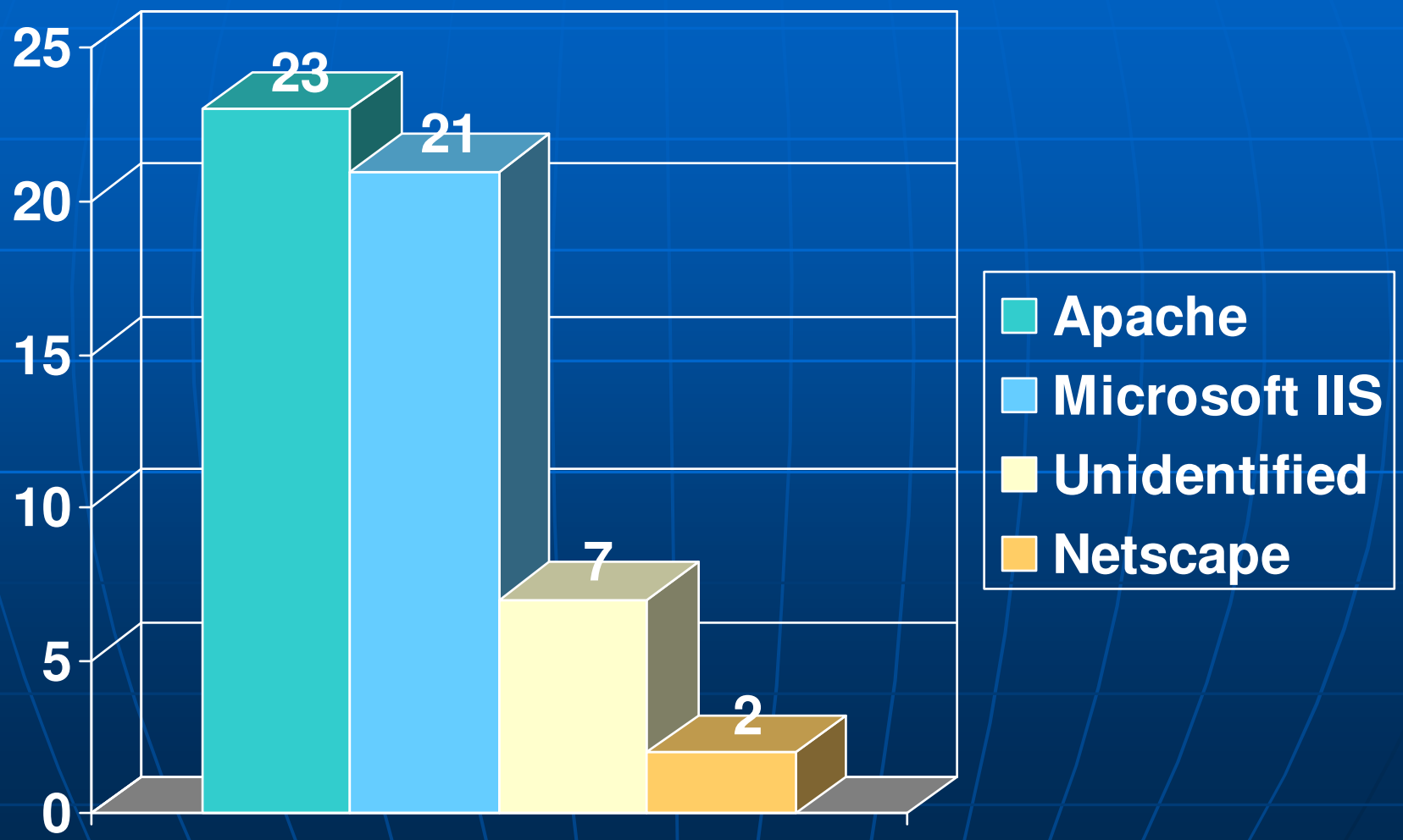


NSPs Info

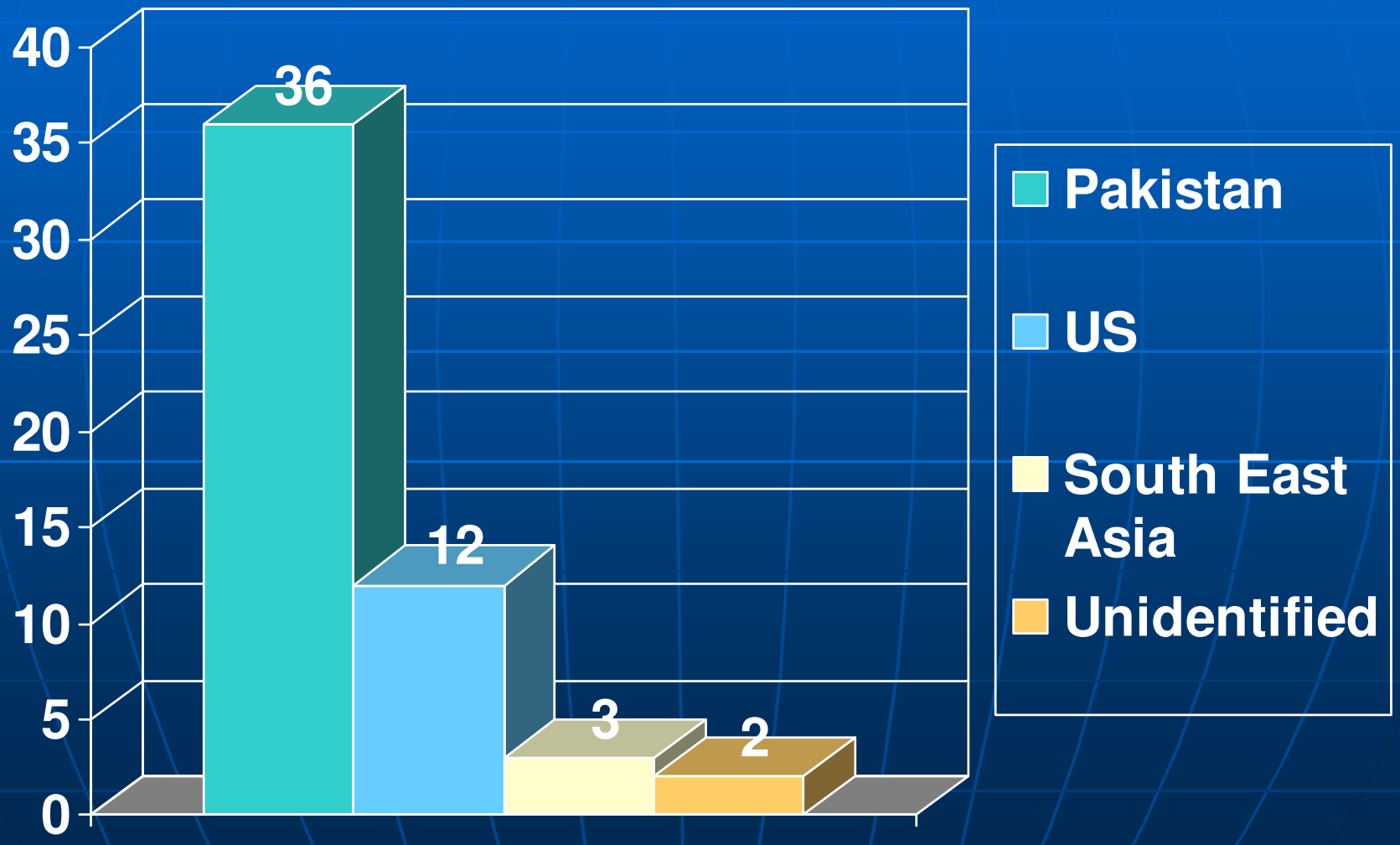
- 53 Network Service Providers

	A	B	C	D	E	F	G	H	
1	ISPs - Internet Service Providers of Pakistan								
2		ISPs	IP Block (Start)	IP Block (End)	IP Address	Country Block (found by IP Address)		Blank = PK	Web Server
3	1	Akunet.org	202.3.130.0	202.3.131.255	202.3.130.3	202.3.130.0	202.3.131.255		Apache/1.3.9 (Unix)
4	2	Amzt.com	202.125.128.0	202.125.159.255 (F	202.125.130.20	202.125.128.0	202.125.159.255		Apache/2.0.44 (Unix) PHP/4
5	3	Aol.net.pk	66.0.0.0	66.255.255.255 *	66.201.115.97	66.201.64.0	66.201.127.255	US	Microsoft-IIS/5.0 X-Powered-
6	4	Apollo.net.pk	202.165.224.0	202.165.255.255	202.165.227.10	202.165.224.0	202.165.255.255		Microsoft-IIS/5.0
7	5	Att.com	192.0.0.0	192.255.255.255	192.20.5.55	192.20.0.0	192.20.224.255	US	Netscape-Enterprise/4.1
8	6	Beacon.net	203.248.0.0	203.255.255.255	203.251.80.133	203.250.0.0	203.251.255.255	South Korea	Apache
9	7	Best.net.pk	202.125.151.88	202.125.151.95	202.125.151.92	202.125.128.0	202.125.159.255		HTTP/1.0 503 Service Unava squid/2.5.STABLE2-200304
10	8	Brain.net.pk	203.128.0.0	203.128.31.255	203.128.7.10	203.128.4.0	203.128.7.255		Apache/1.3.27 (Unix) (Red- mod_ssl/2.8.12 OpenSSL/0 mod_throttle/3.1.2
11	9	Click.net.pk	202.176.224.0	202.176.255.255	202.176.251.5	202.176.224.0	202.176.255.255	Hong Kong	Apache/1.3.29 (Unix) mod_
12	10	Compol.com	151.0.0.0	151.255.255.255	151.196.228.60	151.196.0.0	151.205.255.255	US	

Web Servers In Use



Serving Through Region



Traceroute

	A	B	C	D	E	F	G	H	I
1	**Traceroute**								
2	**Hop**	**%Loss**	**IP Address**	**Node Name**	**Location**	**Tzone**	**MS**	**Graph**	**Network**
721	0		203.130.11.121	def-r6g8tno5wnb	...				
722	1		192.168.1.25	-	...		118	x-	(private use)
723	2		192.168.1.37	-	...		139	-x	(private use)
724	3		203.130.9.22	super9-line-022.super.net.pk	...		148	-x-	
725	4		203.130.9.21	super9-line-021.super.net.pk	...		146	-x-	
726	5		202.125.131.177	s9-1-4.khi77d1.pie.net.pk	...		185	-x--	
727	6		202.125.128.163	g3-0.khi77c1.pie.net.pk	...		200	-x---	
728	7		202.125.159.2	p4-0-0.lhr63c1.pie.net.pk	?(Pakistan)	+05:00	216	--x--	Pakistan Telecommunication Company Limited
729	8		202.125.138.162	lhr63.pie.net.pk	?(Pakistan)	+05:00	237	--x---	Pakistan Telecommunication Company Limited
730	9		202.125.139.46	lhr63.pie.net.pk	?(Pakistan)	+05:00	210	-x---	Pakistan Telecommunication Company Limited
731	10		202.154.224.36	**Wol.net.pk**	?(Pakistan)	+05:00	228	-x-	CyberSoft Technologies Plc

IP Resolution

	A	B	C	D	E	F
1	**Resolved IP Addresses**					
2	**CyberNet**					
3	**Host**	**IP**		**Host**	**IP**	
4	smtp.cyber.net.pk	202.163.96.5		detector.cyber.net.pk	202.163.96.75	
5	ns1.cyber.net.pk	202.163.96.4		angel.cyber.net.pk	202.163.96.76	
6	ns.cyber.net.pk	202.163.96.3		intruzion.cyber.net.pk	202.163.96.78	
7	antivirus.cyber.net.pk	202.163.96.6		security.cyber.net.pk	202.163.96.82	
8	sniffer.cyber.net.pk	202.163.96.8		nms.cyber.net.pk	202.163.96.89	
9	e3000.cyber.net.pk	202.163.96.9		knowledge.cyber.net.pk	202.163.96.90	
10	sniffer2.cyber.net.pk	202.163.96.7		ftp.cyber.net.pk	202.163.96.138	
11	datacenter2.cyber.net.pk	202.163.96.10		hqnotes.cyber.net.pk	202.163.96.166	
12	smtp2.cyber.net.pk	202.163.96.18		cybernt.cyber.net.pk	202.163.96.168	
13	datacenter1.cyber.net.pk	202.163.96.11		bluefin.cyber.net.pk	202.163.96.169	
14	rhino.cyber.net.pk	202.163.96.14		datacenter3.cyber.net.pk	202.163.96.180	
15	webmail.cyber.net.pk	202.163.96.15		proxy9.cyber.net.pk	202.163.96.145	
16	conman.cyber.net.pk	202.163.96.21		arena.cyber.net.pk	202.163.96.170	
17	smtp1.cyber.net.pk	202.163.96.43		dexter.cyber.net.pk	202.163.96.171	
18	antivirus1.cyber.net.pk	202.163.96.35		www.cyber.net.pk	202.163.96.185	
19	denver.cyber.net.pk	202.163.96.52		oldsniffer.cyber.net.pk	202.163.96.190	
20	flamingo.mercury.net.pk	202.163.96.51		relay.cyber.net.pk	202.163.96.133	
21	chkpnt.cyber.net.pk	202.163.96.68		ns4.cyber.net.pk	202.163.96.142	
22	snort.cyber.net.pk	202.163.96.72		ns3.cyber.net.pk	202.163.96.143	
23	datacenter3.cyber.net.pk	202.163.96.71		penguin.cyber.net.pk	202.163.96.242	
24	test.cyber.net.pk	202.163.97.78				

HTTP Info

12		Web Servers					
13		IP	Hostname	Port	Code	Auth	Server
81		SATNet					
82	1	202.133.64.19	mail.hbfc.com.pk	80	200	None	Apache/1.3.27 (Unix)
83	2	202.133.64.213	[Unknown]	80	401	Basic	ZOT-828/2.01
84	3	202.133.64.26	[Unknown]	80	403	None	Microsoft-IIS/5.0
85	4	202.133.64.5	www.sat.net.pk	80	200	None	Apache/1.3.27 (Unix)
86	5	202.133.64.51	[Unknown]	80	200	None	[Unknown]
87	6	202.133.64.10	nms.sat.net.pk	80	401	Basic	Apache/1.3.22 (Unix)
88	7	202.133.64.2	pop.sat.net.pk	80	200	None	Apache/1.3.27 (Unix)
89	8	202.133.64.7	oracle.sat.net.pk	443	400	None	Apache/1.3.12 (Unix) ApacheJServ/1.1 mod_ssl/2.6.4 OpenSSL/0.9.5a mod_perl/1.22
90	9	202.133.64.133	[Unknown]	1214	404	None	[Unknown]
91	10	202.133.64.51	[Unknown]	2779	0	None	[Unknown]
92	11	202.133.64.250	[Unknown]	3128	0	None	[Unknown]
93	12	202.133.64.67	[Unknown]	5000	400	None	[Unknown]
94	13	202.133.64.141	[Unknown]	5000	400	None	[Unknown]
95	14	202.133.64.24	download.sat.net.pk	8888	404	None	Microsoft-IIS/5.0
96	15	202.133.64.26	[Unknown]	8888	404	None	Microsoft-IIS/5.0

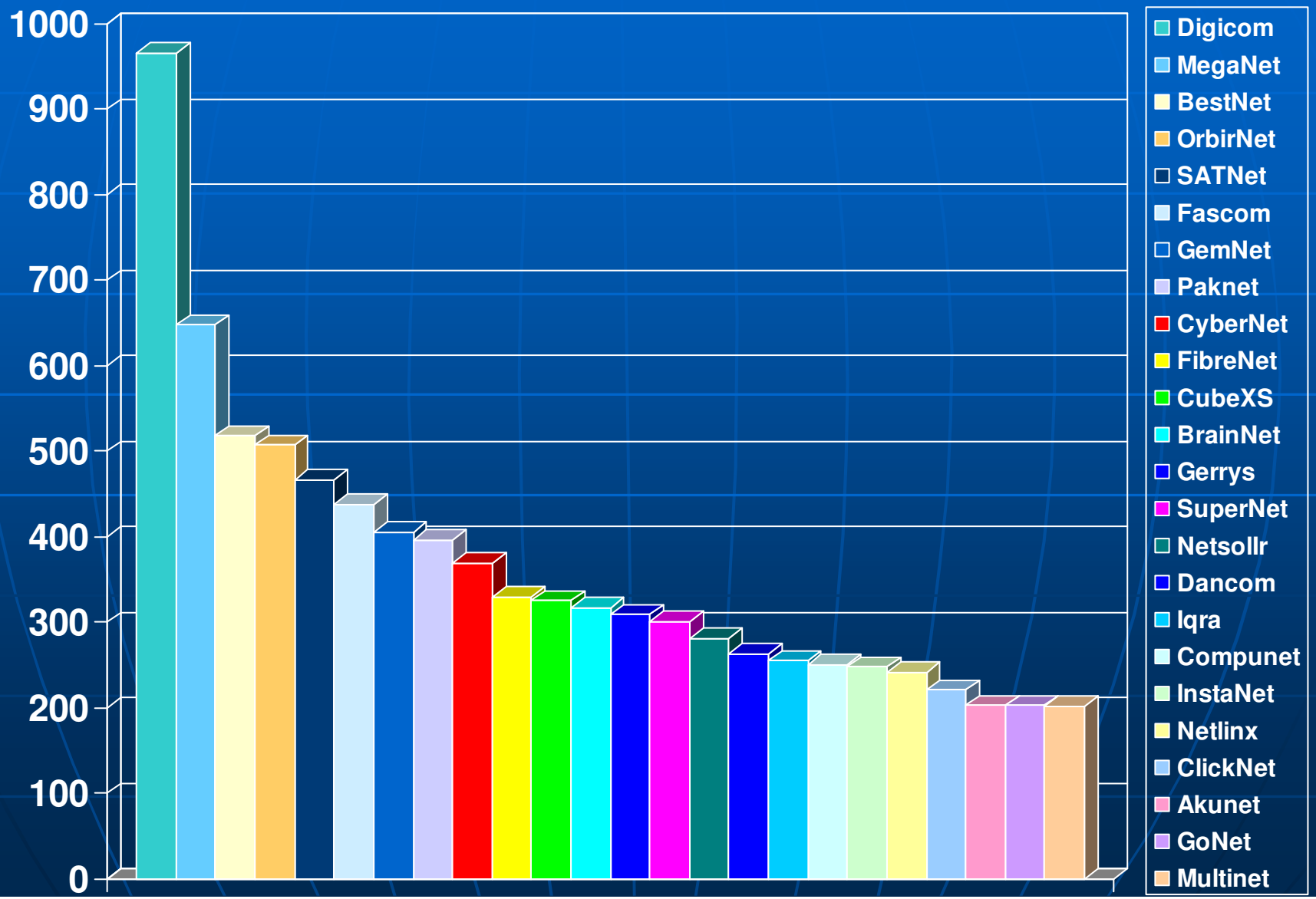
SNMP

	A	B	C	D	E
1	**SNMP - Simple Network Management Protocol**				
2	SuperNet				
3	SATNet				
4	**IP**	**Ports**	**String**	**Response**	
5	**SuperNet**				
6	203.130.2.12	161	public	Linux help 2.2.16-22smp #1 SMP Tue Aug 22 16:39:21 EDT 2000 i686	
7	203.130.2.34	161	public	Cisco Internetwork Operating System Software ..IOS (tm) 7200 Software (C7200-G5IS-M), Version 12.2(1a)XC4, RELEASE SOFTWARE (fc1)..TAC Support: http://www.cisco.com/tac..TAC:Home:Software:Ios General:CiscoIOSRoadmap:12.2(1a)XC2..Copyright (c) 1986-2002 b	
8	203.130.2.129	161	public	HP ETHERNET MULTI-ENVIRONMENT,ROM A.03.17,JETDIRECT,JD24,EEPROM A.04.09	
9	203.130.2.178	161	public	Hardware: x86 Family 15 Model 2 Stepping 4 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 Multiprocessor Free)	
10	203.130.2.249	161	public	Cisco Internetwork Operating System Software ..IOS (tm) C2600 Software (C2600-I-M), Version 12.0(10), RELEASE SOFTWARE (fc1)..Copyright (c) 1986-2000 by cisco Systems, Inc...Compiled Mon 20-Mar-00 23:30 by phanguye	
11	203.130.2.250	161	public	Cisco Internetwork Operating System Software ..IOS (tm) 7200 Software (C7200-G5IS-M), Version 12.2(1a)XC4, RELEASE SOFTWARE (fc1)..TAC Support: http://www.cisco.com/tac..TAC:Home:Software:Ios General:CiscoIOSRoadmap:12.2(1a)XC2..Copyright (c) 1986-2002 b	
12	203.130.2.34	161	private	Cisco Internetwork Operating System Software ..IOS (tm) 7200 Software (C7200-G5IS-M), Version 12.2(1a)XC4, RELEASE SOFTWARE (fc1)..TAC Support: http://www.cisco.com/tac..TAC:Home:Software:Ios General:CiscoIOSRoadmap:12.2(1a)XC2..Copyright (c) 1986-2002 b	
13	203.130.2.129	161	private	HP ETHERNET MULTI-ENVIRONMENT,ROM A.03.17,JETDIRECT,JD24,EEPROM A.04.09	
14	203.130.2.250	161	private	Cisco Internetwork Operating System Software ..IOS (tm) 7200 Software (C7200-G5IS-M), Version 12.2(1a)XC4, RELEASE SOFTWARE (fc1)..TAC Support: http://www.cisco.com/tac..TAC:Home:Software:Ios General:CiscoIOSRoadmap:12.2(1a)XC2..Copyright (c) 1986-2002 b	
15					
16	**SatNet**				
17	202.133.65.54	161	public	Hardware: x86 Family 6 Model 8 Stepping 1 AT/AT COMPATIBLE - Software: Windows 2000 Version 5.1 (Build 2600 Uniprocessor Free)	

DNS

	A	B	C	D
1	DNS Qeuery Results for Pakistan's Official Sites (.GOV)			
2	A, AXFR, CNAME, HINFO, MAILB, MB, MG, MINFO, MR, MX, NS, PTR, RP, SOA, TXT, WKS,			
190	Header:			
191	ID=20427	QR=Response	Opcode=QUERY	RCODE=NO ERROR
192	Authoritative Answer=No	Truncation=No		
193	Recursion Desired=Yes	Recursion Available=Yes		
194	QDCOUNT=1	ANCOUNT=1	NSCOUNT=2	ARCOUNT=2
195	Question:			
196	**name(=)www.cbr.gov.pk**	QTYPE=ALL	QCLASS=1	
197	Answer Section:			
198	- name(=)www.cbr.gov.pk			
199	Type=A	Class=1	TTL=76807 (21 Hours 20 Minutes 7 Seconds)	RDLENGTH=4
200	IP Address=66.201.122.3			
201	Authority Records Section:			
202	- name(=)cbr.gov.pk			
203	Type=NS	Class=1	TTL=76807 (21 Hours 20 Minutes 7 Seconds)	RDLENGTH=18
204	Name Server=ns1.cybercon.com			
205	- name(=)cbr.gov.pk			
206	Type=NS	Class=1	TTL=76807 (21 Hours 20 Minutes 7 Seconds)	RDLENGTH=6
207	Name Server=ns2.cybercon.com			
208	Additional Records Section:			
209	- name(=)ns1.cybercon.com			
210	Type=A	Class=1	TTL=1366 (22 Minutes 46 Seconds)	RDLENGTH=4
211	IP Address=216.15.129.2			
212	- name(=)ns2.cybercon.com			
213	Type=A	Class=1	TTL=75891 (21 Hours 4 Minutes 51 Seconds)	RDLENGTH=4
214	IP Address=216.15.129.3			
215	---			

Services (Range 1 → 139)



Services (Range 1 → 139) Cont…

	A	B	C	D
1	Services Index (ISPs hyperlinked)			
2		ISP	Services	
3		Digicom	966	
4		MegaNet	648	
5		BestNet	518	
6		OrbirNet	507	
7		SATNet	467	
8		Fascom	438	
9		GemNet	406	
10		Paknet	397	
11		CyberNet	369	
12		FibreNet	330	
13		CubeXS	325	
14		BrainNet	317	
15		Gerrys	309	
16		SuperNet	301	
17		Netsollr	281	
18		Dancom	263	
19		Iqra	255	
20		Compunet	251	
21		InstaNet	248	
22		Netlinx	242	
23		ClickNet	221	
24		Akunet	203	
25		GoNet	203	
26		Multinet	202	
27			8667	
28				

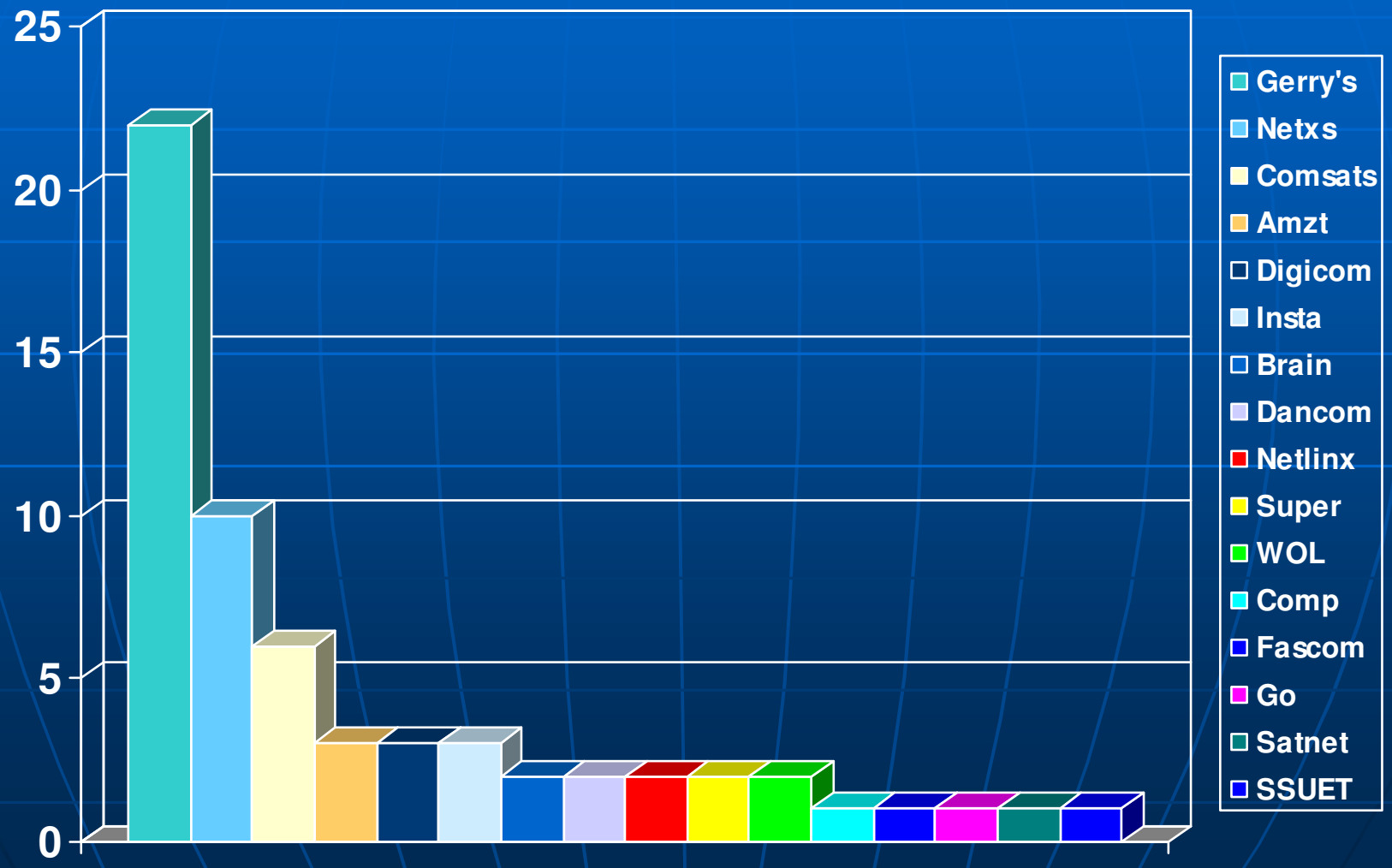
Count - ISP Wise

	A	B	C	D	E
1	**Services (Class C scanned for ports 1-139)**				
2	TOC	Services Index			
3	**Sr No**	**IP**	**Port**	**Host Name**	**Protocol**
960	184	202.163.96.191	1	tcpmux	TCPPortServiceMultiplexer
961	185	202.163.96.191	2	compressnet	ManagementUtility
962	186	202.163.96.191	3	compressnet	CompressionProcess
963	187	202.163.96.191	4	#	Unassigned
964	188	202.163.96.191	5	rje	RemoteJobEntry
965	189	202.163.96.191	6	#	Unassigned
966	190	202.163.96.191	7	echo	Echo
967	191	202.163.96.191	8	#	Unassigned
968	192	202.163.96.191	9	discard	Discard
969	193	202.163.96.191	10	#	Unassigned
970	194	202.163.96.191	11	systat	ActiveUsers
971	195	202.163.96.191	12	#	Unassigned
972	196	202.163.96.191	13	daytime	Daytime(RFC867)
973	197	202.163.96.191	14	#	Unassigned
974	198	202.163.96.191	15	#	Unassigned[wasnetstat]
975	199	202.163.96.191	16	#	Unassigned
976	200	202.163.96.191	17	qotd	QuoteoftheDay
977	201	202.163.96.191	18	msp	MessageSendProtocol
978	202	202.163.96.191	19	chargen	CharacterGenerator
979	203	202.163.96.191	20	ftp-data	FileTransfer[DefaultData]
980	204	202.163.96.191	21	ftp	FileTransfer[Control]
981	205	202.163.96.191	22	ssh	SSHRemoteLoginProtocol
982	206	202.163.96.191	23	telnet	Telnet
983	207	202.163.96.191	24	any	privatemailsystem
984	208	202.163.96.191	25	smtp	SimpleMailTransfer

Count - Services Wise

	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Service wise totals												
2	Port	Service	Total	SatNet	SuperNet	CyberNet	Fascom	CubeXS	Akunet	BrainNet	Dancom	CompuNet	GemNet
3	1	TCPPortServiceMultiplexer	6	0	0	1	0	0	0	1	0	0	1
4	2	ManagementUtility	2	0	0	1	0	0	0	0	0	0	0
5	3	CompressionProcess	2	0	0	1	0	0	0	0	0	0	0
6	4	Unassigned	2	0	0	1	0	0	0	0	0	0	0
7	5	RemoteJobEntry	2	0	0	1	0	0	0	0	0	0	0
8	6	Unassigned	2	0	0	1	0	0	0	0	0	0	0
9	7	echoEcho	124	6	1	2	0	6	0	2	1	0	2
10	8	Unassigned	2	0	0	1	0	0	0	0	0	0	0
11	9	Discard	123	6	1	2	0	6	0	2	1	0	2
12	10	Unassigned	2	0	0	1	0	0	0	0	0	0	0
13	11	ActiveUsers	3	0	0	1	0	0	0	0	0	0	1
14	12	Unassigned	2	0	0	1	0	0	0	0	0	0	0
15	13	daytimeDaytime(RFC867)	115	5	1	2	0	6	0	2	1	0	1
16	14	Unassigned	2	0	0	1	0	0	0	0	0	0	0
17	15	Unassigned[wasnetstat]	3	0	0	1	0	0	0	0	0	0	1
18	16	Unassigned	2	0	0	1	0	0	0	0	0	0	0
19	17	qotdQuoteoftheDay	113	2	1	2	0	6	0	2	1	0	0
20	18	MessageSendProtocol	2	0	0	1	0	0	0	0	0	0	0
21	19	CharacterGenerator	119	5	1	2	0	7	0	2	1	0	1
22	20	FileTransfer[DefaultData]	2	0	0	1	0	0	0	0	0	0	0
23	21	FileTransfer[Control]	506	159	10	5	0	0	0	9	14	1	68
24	22	SSHRemoteLoginProtocol	151	2	4	3	1	0	0	0	3	1	1
25	23	Telnet	138	8	10	3	8	0	0	22	17	4	0
26	24	privatemailsystem	3	0	0	1	0	0	0	0	0	0	0
27	25	smtpSimpleMailTransfer	410	12	17	4	70	7	4	16	6	1	70
28	26	Unassigned	4	0	0	1	0	0	0	0	0	0	0
29	27	NSWUserSystemFE	4	0	1	1	0	0	0	1	0	0	0
30	28	Unassigned	3	0	0	1	0	0	0	0	0	0	0
31	29	MSGICP	2	0	0	1	0	0	0	0	0	0	0

Vulnerable (Apache Chunked)



Specific Examples

Comprehensive Report

- An ISP giving out SNMP and vulnerability info

Scan target : **203.130.2.1-203.130.2.254** [**21** computers found]

IP Address	Details	Hostname	Username	Operating System
203.130.2.1				probably Unix
203.130.2.3				probably Unix
203.130.2.4				probably Unix
203.130.2.6				probably Unix
203.130.2.7				probably Unix
203.130.2.9				probably Unix
203.130.2.11				Windows
203.130.2.12		help		Linux
203.130.2.13				probably Unix
203.130.2.15				Windows
203.130.2.16				probably Unix
203.130.2.17				probably Unix
203.130.2.18				Windows
203.130.2.27				Windows
203.130.2.28				Windows
203.130.2.29				probably Unix
203.130.2.34		TCL		Cisco 7206 VXR
203.130.2.41				undetermined
203.130.2.129				HP Jet-Direct Print Server
203.130.2.178		EXCHANGE		2K Server
203.130.2.250		TCL		undetermined

Comprehensive Report (Cont…)

- State of an ISP

IP Address	Details	Hostname	Username	Operating System
203.130.2.17				probably Unix

203.130.2.17 [ ] probably Unix

IP Address : **203.130.2.17**
Resolved : **khayal.super.net.pk**
Operating System : **probably Unix**

Alerts

FTP alerts

Ftp Exposing Full Path

Anonymous FTP is exposing full path. This might give out sensitive information or mean that the ftp server is misconfigured.

Mail alerts

Remote Buffer Overflow in Sendmail

Sendmail versions from 5.79 to 8.12.7 are vulnerable to this buffer overflow.
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1337

Service alerts

Telnet service is running

This service is dangerous because it doesn't encrypt data. Sensitive information (usernames+passwords) can be sniffed. If possible use SSH instead.

Comprehensive Report (Cont…)

- SNMP Details

202.147.176.251 [gwpsh] Cisco 2620

IP Address : **202.147.176.251**
Hostname : **gwpsh**
Operating System : **Cisco 2620**
Time to live : **0**

SNMP info (system)

sysDescr - Cisco Internetwork Operating System Software __IOS (tm) C2600 Software (C2600-IS-M), Version 12.0(5)T1, RELEASE SOFTWARE (fc1)__Copyright (c) 1986-1999 by cisco Systems, Inc.__Compiled Tue 17-Aug-99 14:39 by cmong
sysUpTime - 6 days, 2 hours, 50 minutes, 17 seconds
sysName - gwpsh
Object ID - 1.3.6.1.4.1.9.1.208 (Cisco 2620)
Vendor - cisco

Comprehensive Report (Cont…)

- An educational institute running a Trojan

Scan target : **www.bol.edu.pk** [**1** computers found]

IP Address	Details	Hostname	Username	Operating System
202.5.149.3				Windows

202.5.149.3 [ ] Windows

IP Address : **202.5.149.3**
Operating System : **Windows**
Time to live : **128**

TCP ports - 1 open ports
1045 [RASmin]

Alerts
Backdoors
RASmin (1045)

Individuals' Info

- Users of an ISP

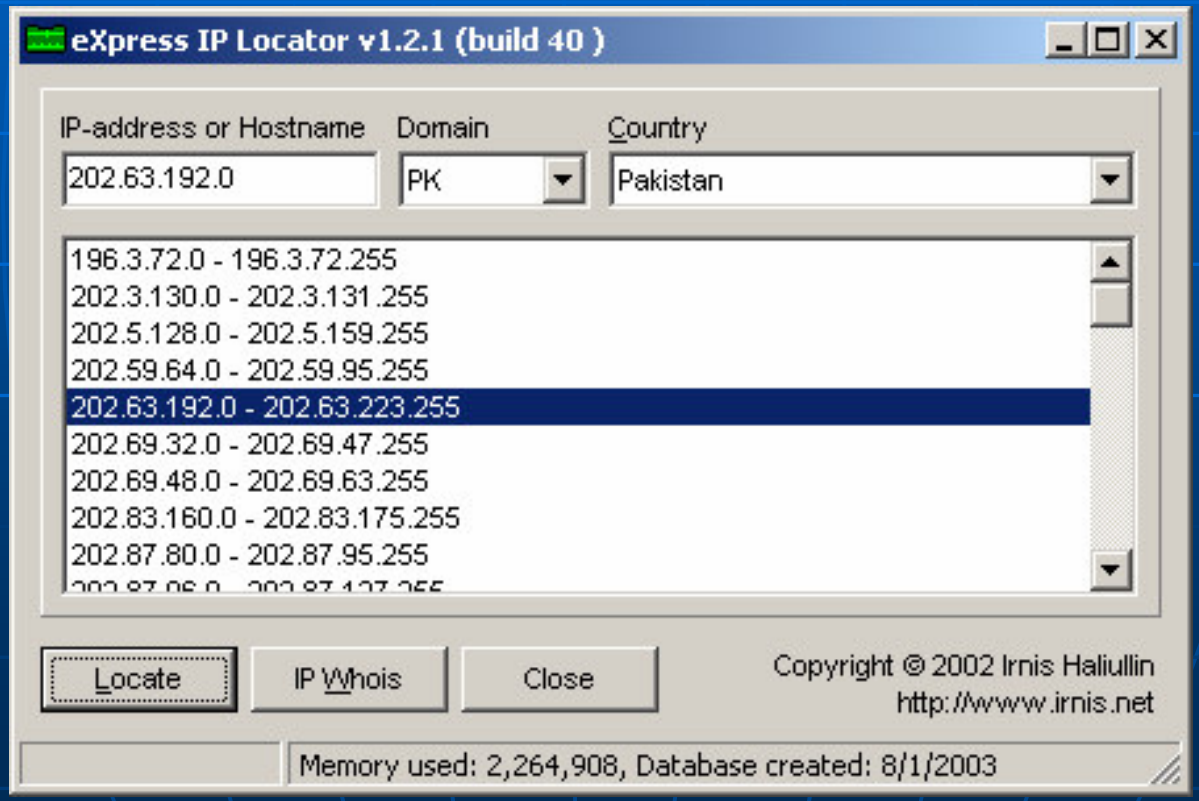
IP Address	Details	Hostname	Username
202.125.133.5			(No one logged on)
202.125.133.8			(No one logged on)
202.125.133.14		D8B1G2	EVERY
202.125.133.15		SUPER	SUPER
202.125.133.17		FAYZ	FAYZ
202.125.133.19		ARIF	ARIF
202.125.133.23		SERVER	(No one logged on)
202.125.133.27			(No one logged on)
202.125.133.30			(No one logged on)
202.125.133.31		DREAMCATCHER	DREAMCATCHER
202.125.133.33			(No one logged on)
202.125.133.35			(No one logged on)
202.125.133.38			(No one logged on)
202.125.133.39		WAQQAS	WAQQAS
202.125.133.40		PENTIIIASAD	PENTIIIASAD
202.125.133.44		AMJADALI	AMJADALI

Tools

- Snapshots of 7 out of more than 215 used

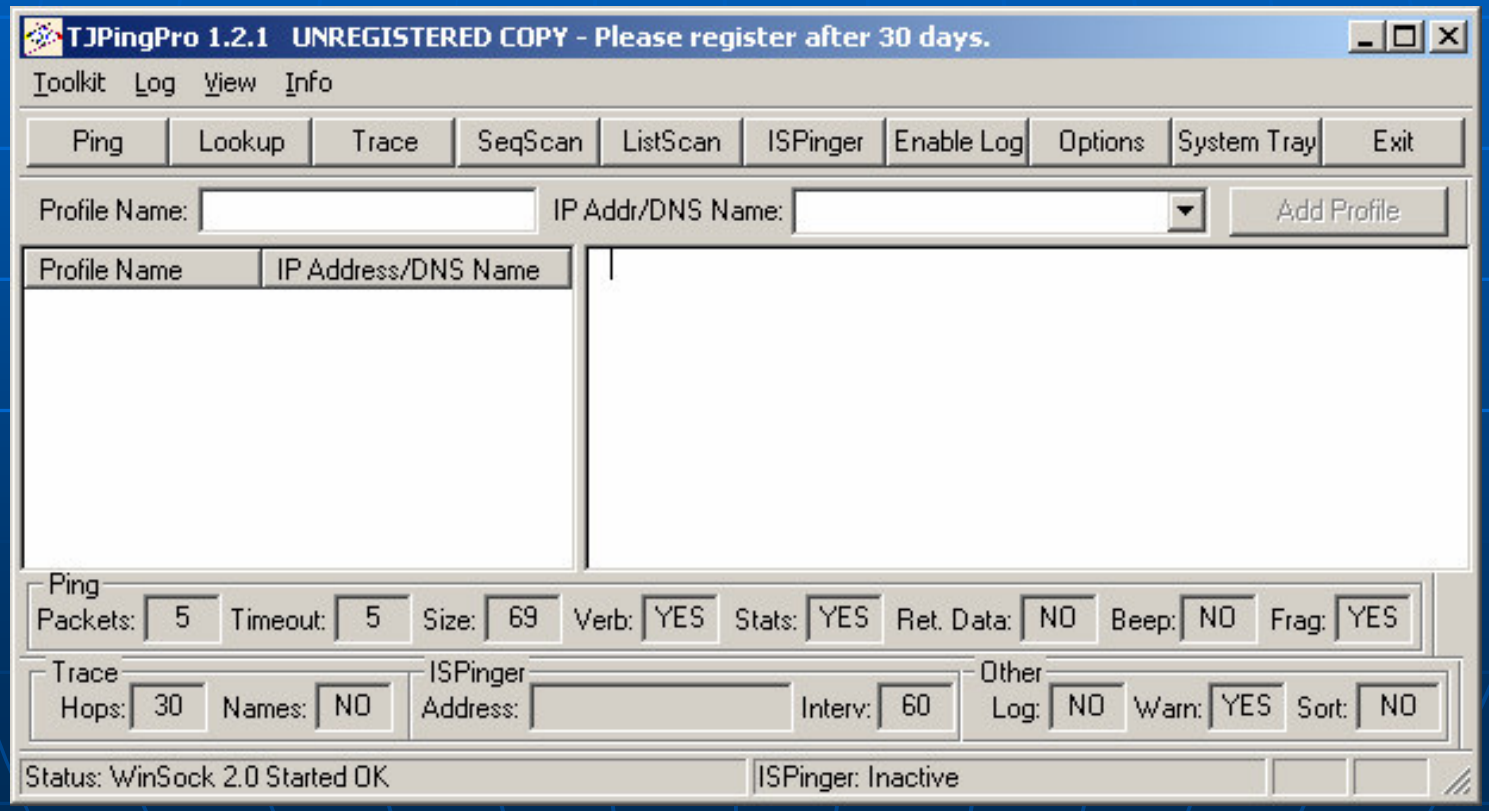
Tools (Cont…)

- Country Info



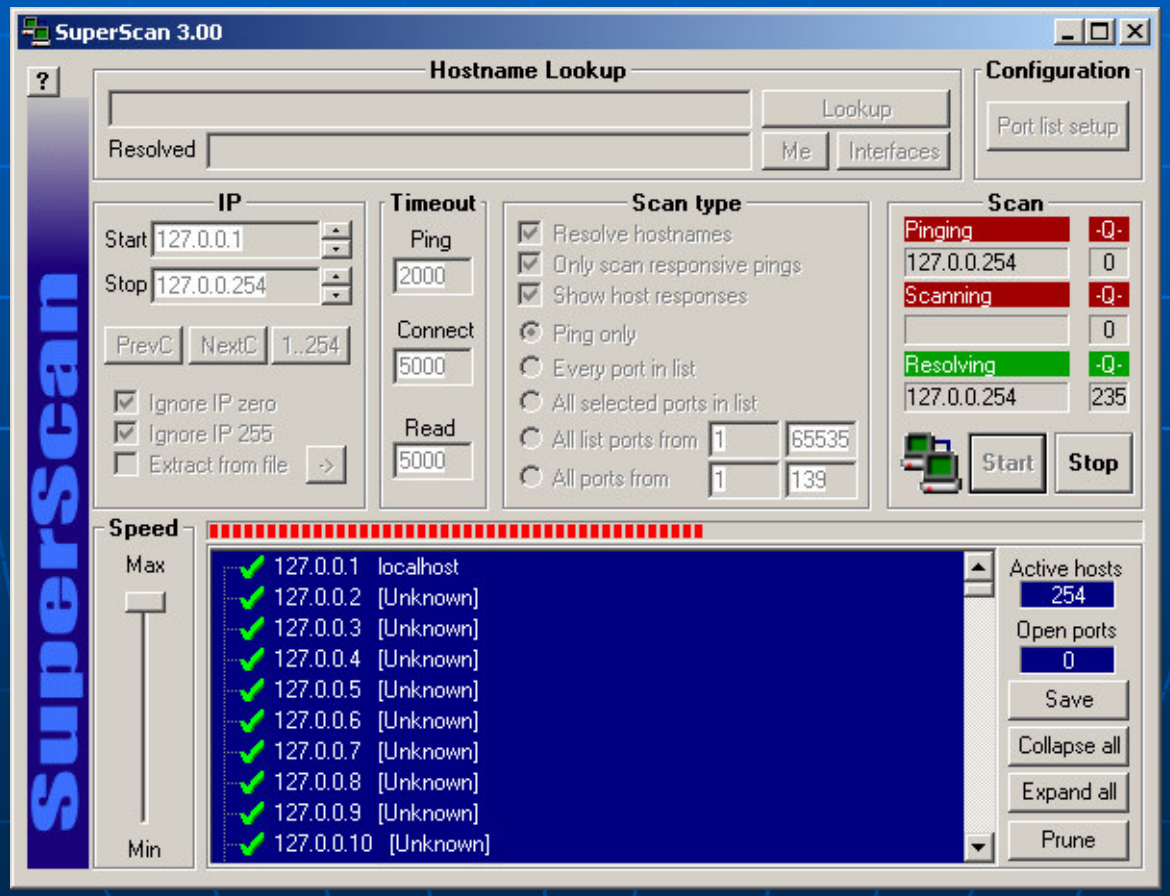
Tools (Cont…)

- Ping



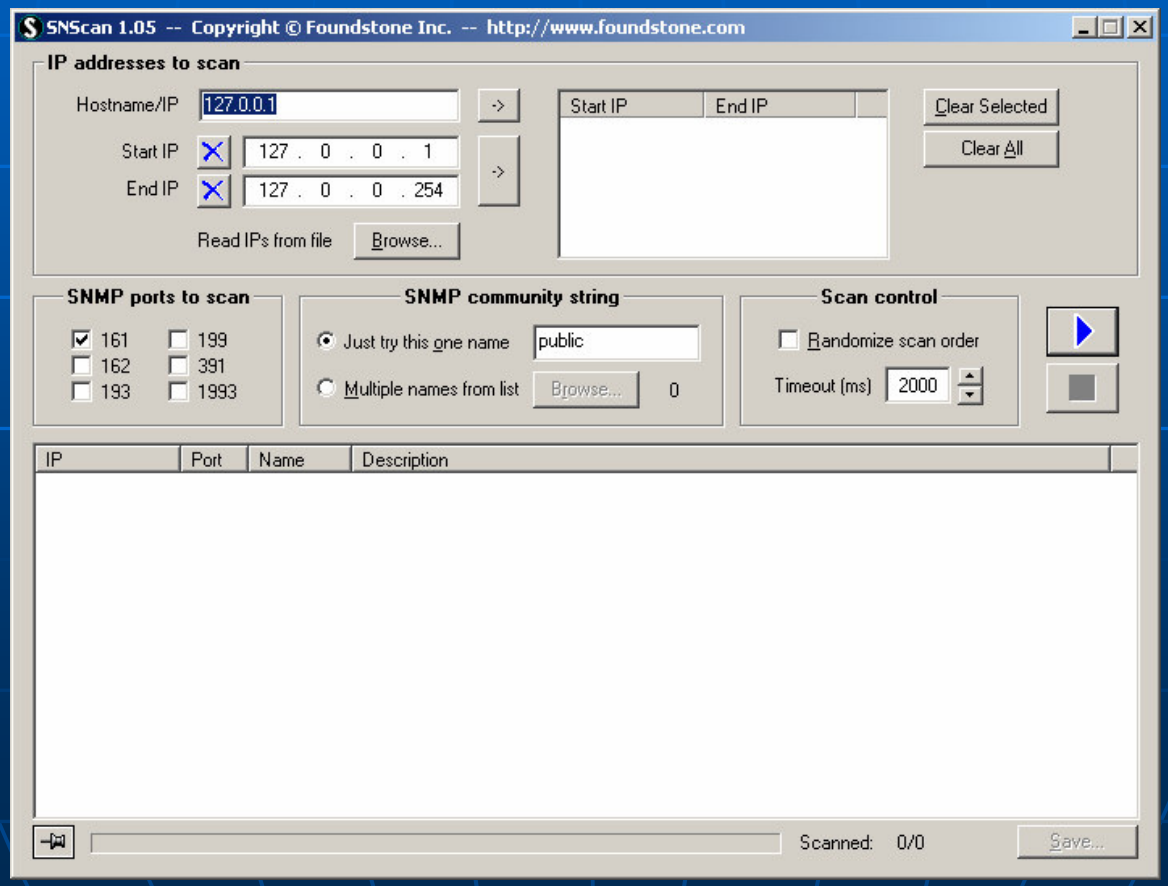
Tools (Cont…)

- Scan



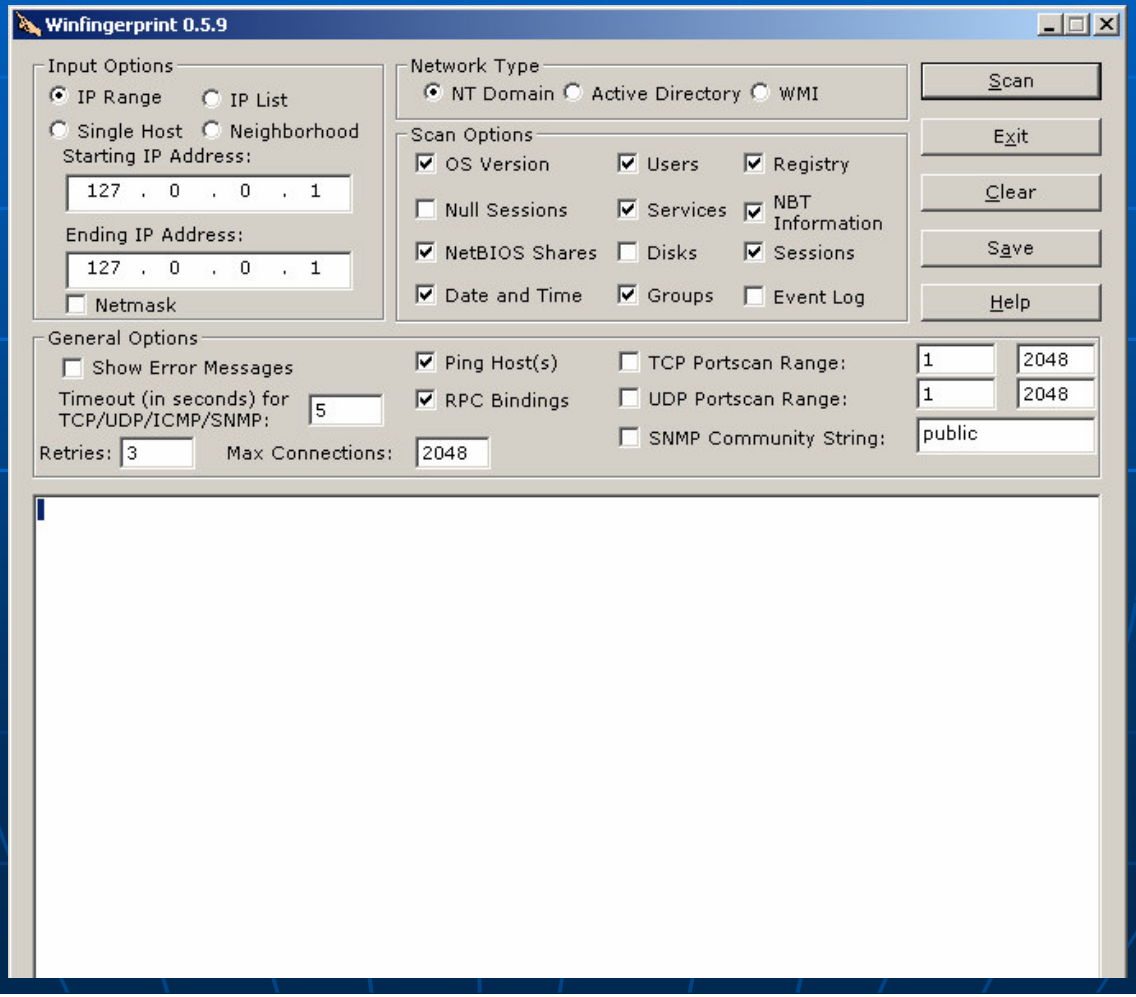
Tools (Cont…)

- SNMP (Can download strings)



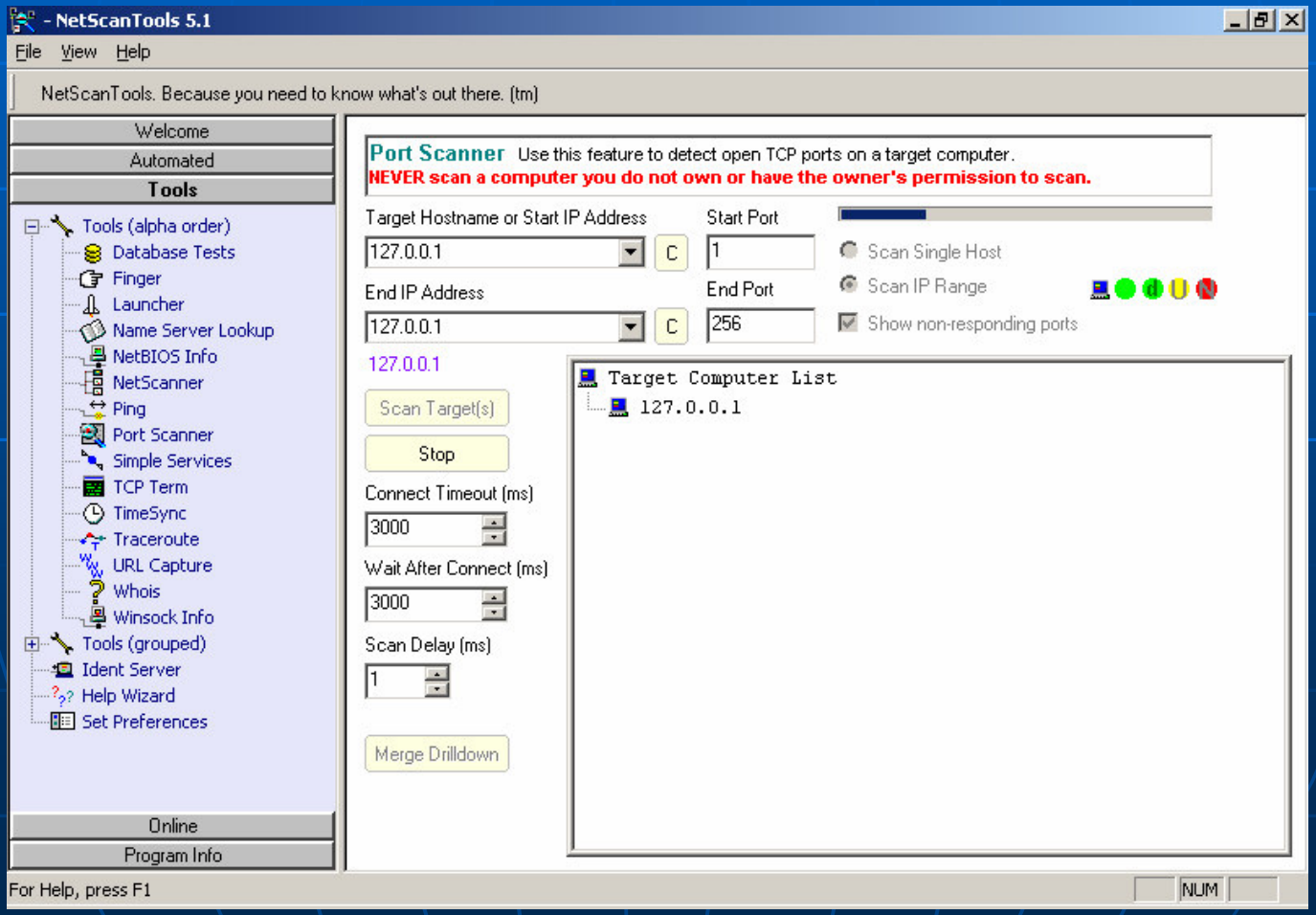
Tools (Cont…)

- Multiple 1



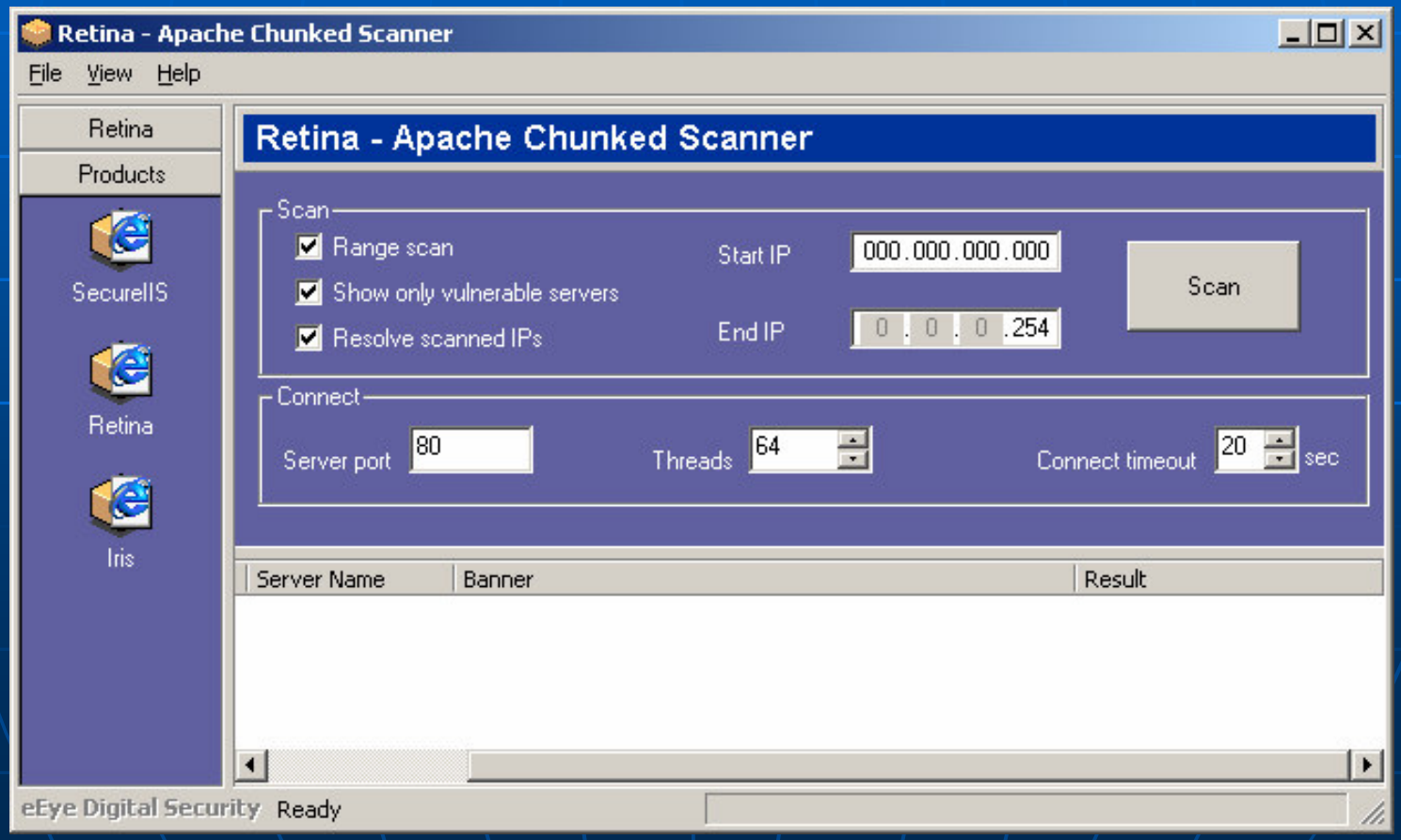
Tools (Cont…)

- Multiple 2



Tools (Cont…)

- Vulnerability Scan



Scale Of Network Activity

- Requests sent only on Port Scan
  23 x 255 x 139 = 850,680
- Services identified
  8,600+
- Tools Used
  215+

Limitations / Scope

- Had limited time and resources
- The amount of data collected and work done is in accordance with the time frame, not with the targets of the study
- Scanning has been performed in the range of 139/65535, on 24/53 NSPs
- Tools used are only for Windows

Recommendations

- Ask NSPs if this information should be available?
- Ask them if they expect others to know this?
- Do we need any legislation for info control?
- This study is only a start – a more rigorous effort would reveal even more info

The End