



# Ethical Hacking and Countermeasures

Version 6



## Module V

## Scanning

Stephen used to be the most bullied guy in his circle of friends. Johnson, the neighborhood guy was part of the peer group and foremost in bullying Stephen. Stephen started developing hatred for Johnson.

Johnson owned/hosted a personal website where he showcased his website development skills. He passed the IP address of his website to his peer group so that they could comment on it after viewing the pages.

Stephen comes across an article on hacking on the Internet. Amazed by the potential of tools showcased in that article, he decides to try it hands on. With the downloaded scanning tools, Stephen started scanning the IP of Johnson's website

*What kind of information will Stephen be exposed to?*

*Will the scan performed by Stephen affect Johnson's Website?*

## Bill Gates says Internet censorship won't work

Robert McMillan

**February 20, 2008** (IDG News Service) Efforts by countries like China to restrict the exchange of information on the Internet are ultimately doomed to failure, Microsoft Chairman Bill Gates told an audience of Stanford University students Tuesday.

"I don't see any risk in the world at large that someone will restrict free content flow on the Internet," he said. "You cannot control the Internet."

China has grappled with the issue of Internet censorship in recent years, and Microsoft Corp., along with several other U.S. companies, has come under fire for aiding in that effort. In late 2005, Microsoft shut down the blog of journalist Zhao Jing, also known as Michael Anti, when he blogged about a newspaper strike in the country.

In the long run, free speech will win out, Gates said.

It will be driven by business requirements. Restrictions on free speech will curtail business activity, and so commercial forces will work against censorship, Gates said. "If your country wants to have a developed economy ... you basically have to open up the Internet," he said.

Gates made the comments following a talk on "software, innovation, entrepreneurship and giving back," which focused mainly on his two favorite topics: the future of technology and the philanthropic goals he has set for himself following his retirement from day-to-day work at the company he founded in 1975.

Microsoft's founder will step down from his daily work at the company entirely in July, but he has set some big follow-up goals for himself, including the fight against HIV/AIDS and a campaign to eradicate polio and malaria.

Another ambition is to find new ways to drive innovation that will benefit the world's poorest countries.

**Pronto**

Discover what Open Communications can deliver now!

Communication for the open minded

**SIEMENS**

Visit Website | Download Survey | View Webinar

Source: <http://www.computerworld.com/> Copyright © by EC-Council

All Rights Reserved. Reproduction is Strictly Prohibited

## Canadian police raid international 'hacker network'

Posted Fri Feb 22, 2008 10:14pm AEDT

**Police in Canada have broken up a major international computer-hacking network.**

The ring targeted unprotected personal computers around the world.

Police raided homes across Quebec arresting 16 people in what authorities describe as the largest hacking scam in Canadian history.

Police say the hackers worked together online to attack and gain control of as many as one million computers worldwide, specifically focusing on those that were not protected with anti-virus software or firewalls.

Once the network gained control, it used the computers to set up fake websites that asked people to click on them to provide personal information.

Police say most of the computers that were attacked were in the US, Poland and Brazil.

They say several government computers were also hacked, but they would not say in which country.

It is estimated that the ring took in as much as \$45 million.

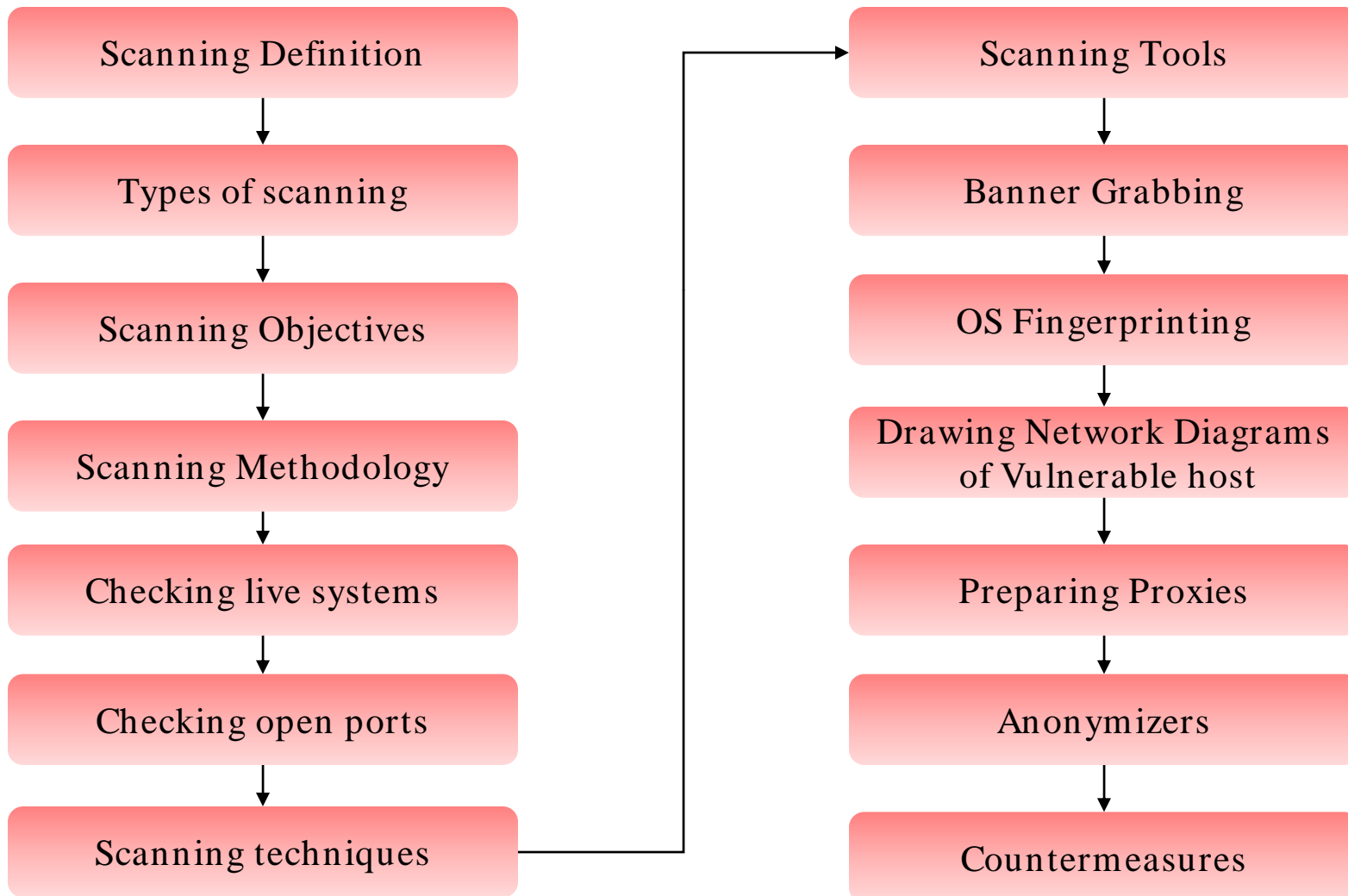
Source: <http://www.abc.net.au/>



This module will familiarize you with:

- Definition of scanning
- Types and objectives of Scanning
- Understanding CEH Scanning methodology
- Checking live systems and open ports
- Understanding scanning techniques
- Different tools present to perform Scanning
- Understanding banner grabbing and OS fingerprinting
- Drawing network diagrams of vulnerable hosts
- Preparing proxies
- Understanding anonymizers
- Scanning countermeasures

# Module Flow



# Scanning - Definition

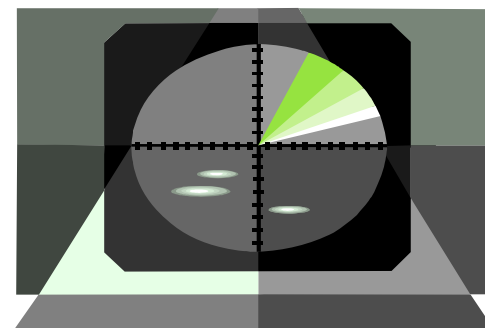
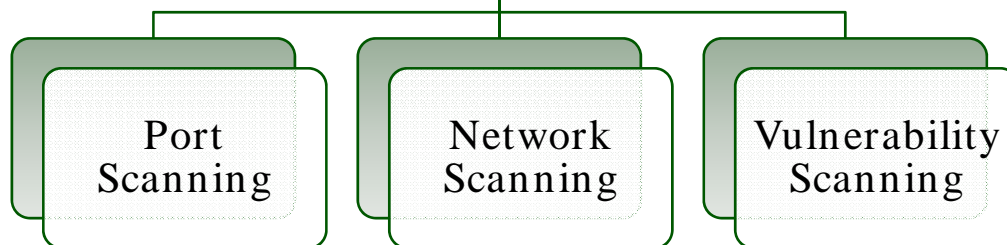
Scanning is one of the three components of intelligence gathering for an attacker

The attacker finds information about the:

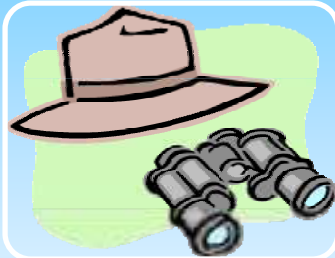
- Specific IP addresses
- Operating Systems
- System architecture
- Services running on each computer



The various types of scanning are as follows:



# Types of Scanning



## Port Scanning

- A series of messages sent by someone attempting to break into a computer to learn about the computer's network services
- Each associated with a "well-known" port number



## Network Scanning

- A procedure for identifying active hosts on a network
- Either for the purpose of attacking them or for network security assessment



## Vulnerability Scanning

- The automated process of proactively identifying vulnerabilities of computing systems present in a network

# Objectives of Scanning



To detect the live systems running on the network

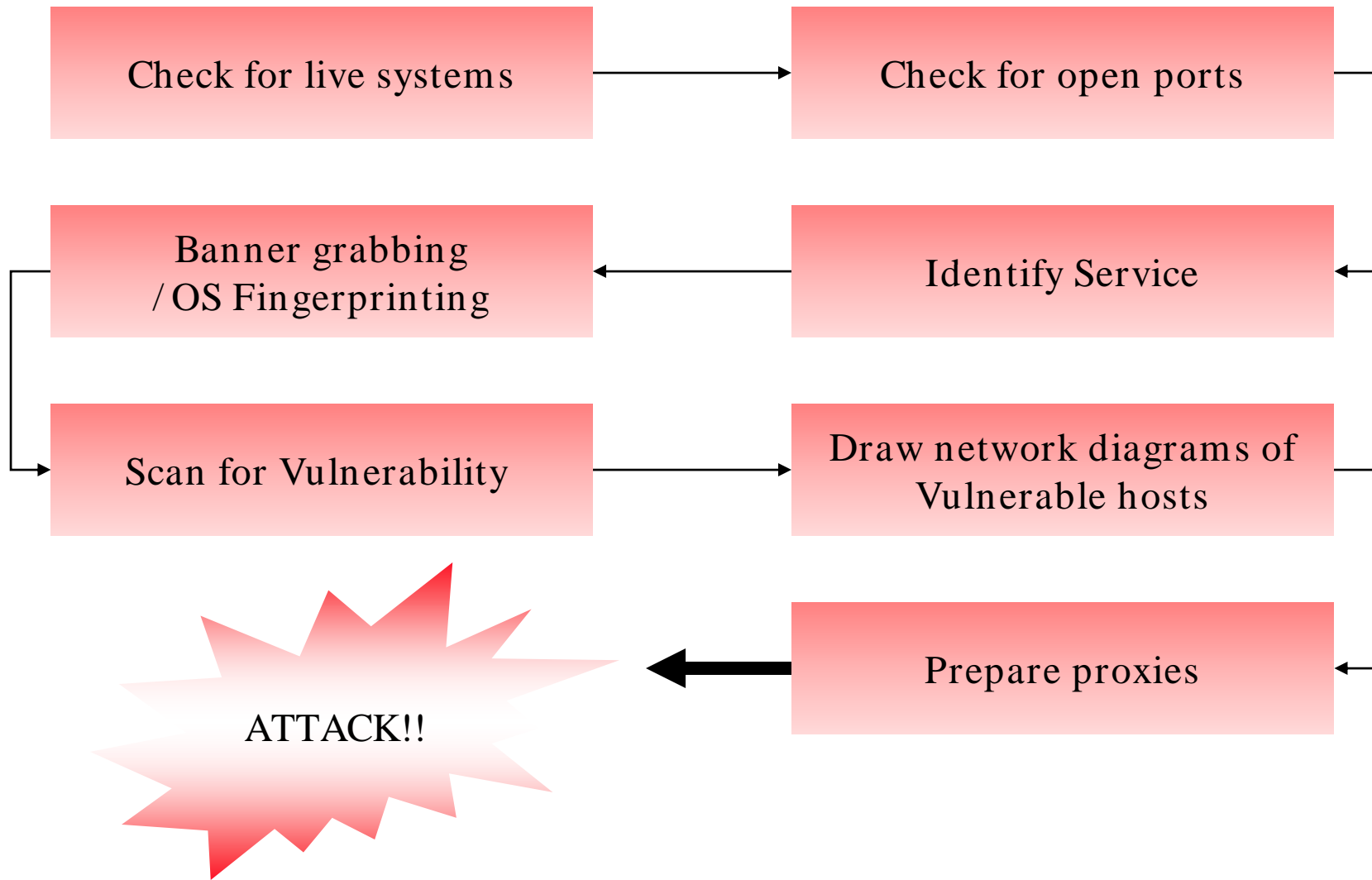
To discover which ports are active/running

To discover the operating system running on the target system (fingerprinting)

To discover the services running/listening on the target system

To discover the IP address of the target system

# CEH Scanning Methodology





# Checking for Live Systems

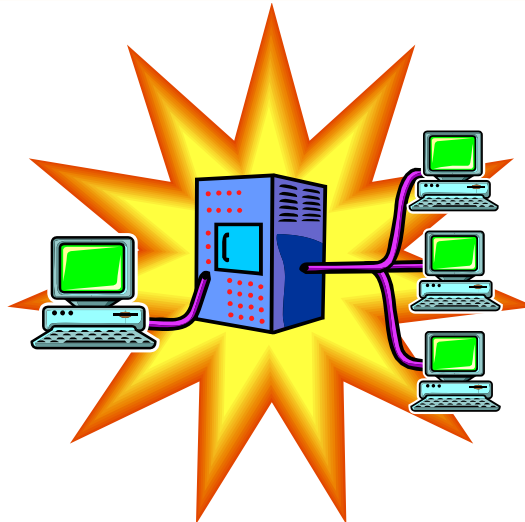


# Checking for Live Systems - ICMP Scanning

In this type of scanning, it is found out which hosts are up in a network by pinging them all

ICMP scanning can be run parallel so that it can run fast

It can also be helpful to tweak the ping timeout value with the `-t` option



# Angry IP Scanner

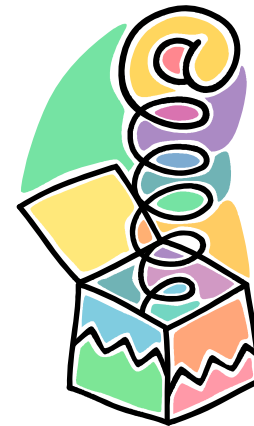
An IP scanner for Windows

Can scan IPs in any range

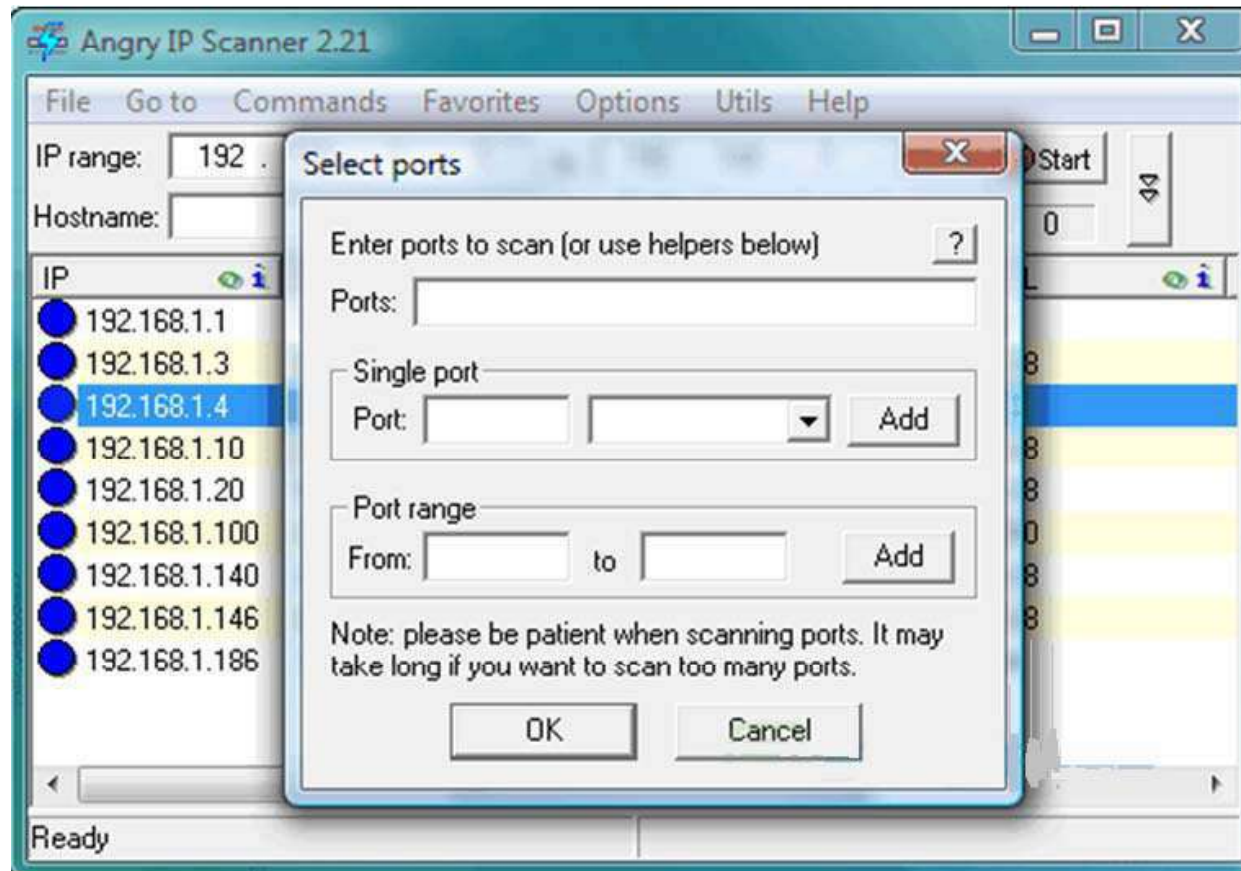
It simply pings each IP address to check if it is alive

Provides NETBIOS information such as:

- Computer name
- Workgroup name
- MAC address



# Angry IP Scanner: Screenshot

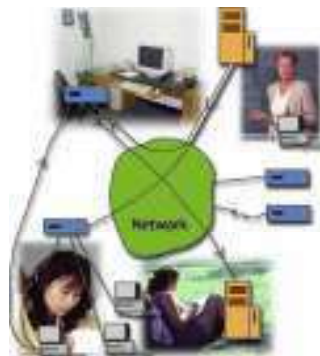


# Ping Sweep

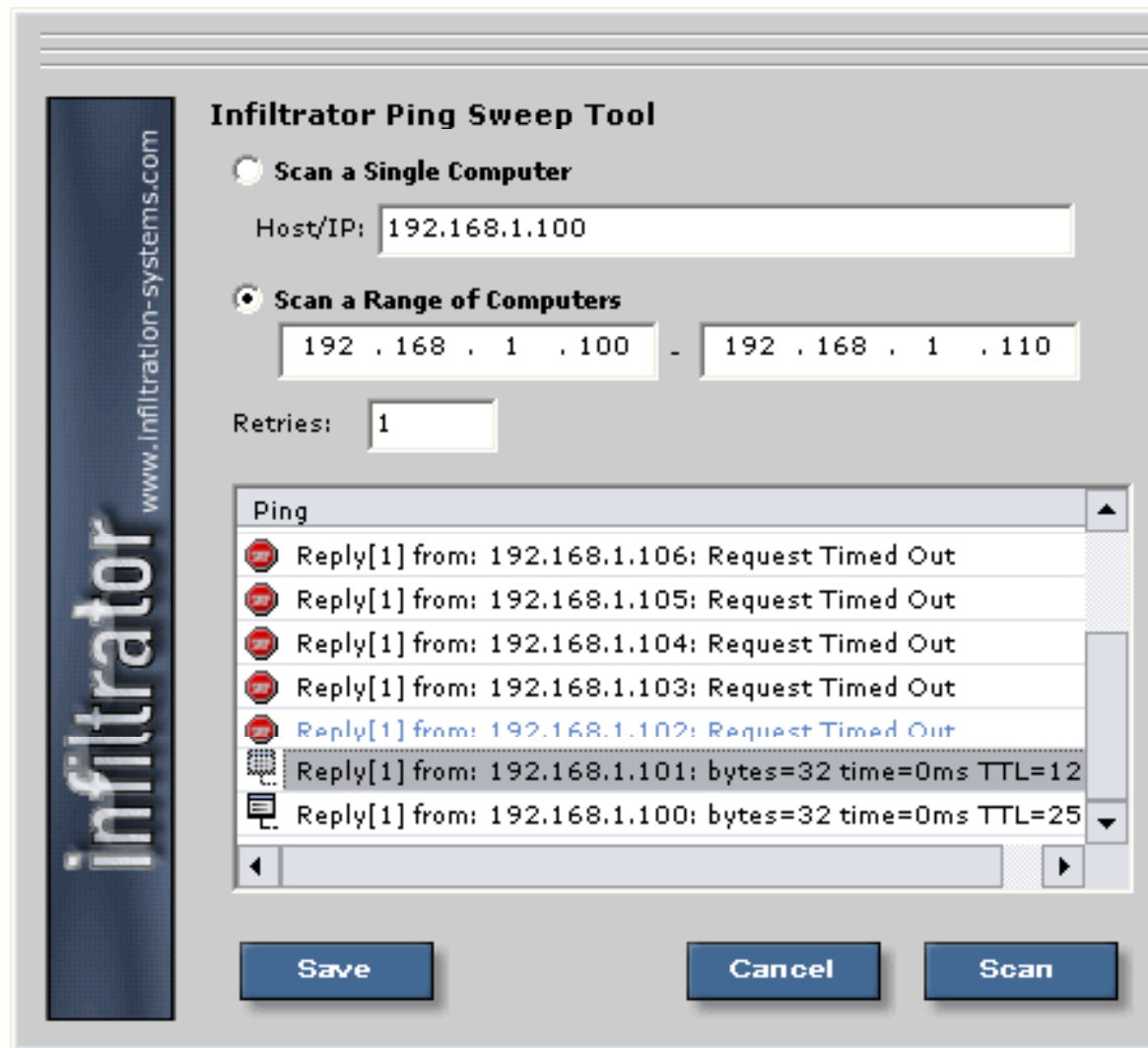
A ping sweep (also known as an ICMP sweep) is a basic network scanning technique used to determine which of a range of IP addresses map to live hosts (computers)

A ping sweep consists of ICMP ECHO requests sent to multiple hosts

If a given address is live, it will return an ICMP ECHO reply



# Ping Sweep: Screenshot



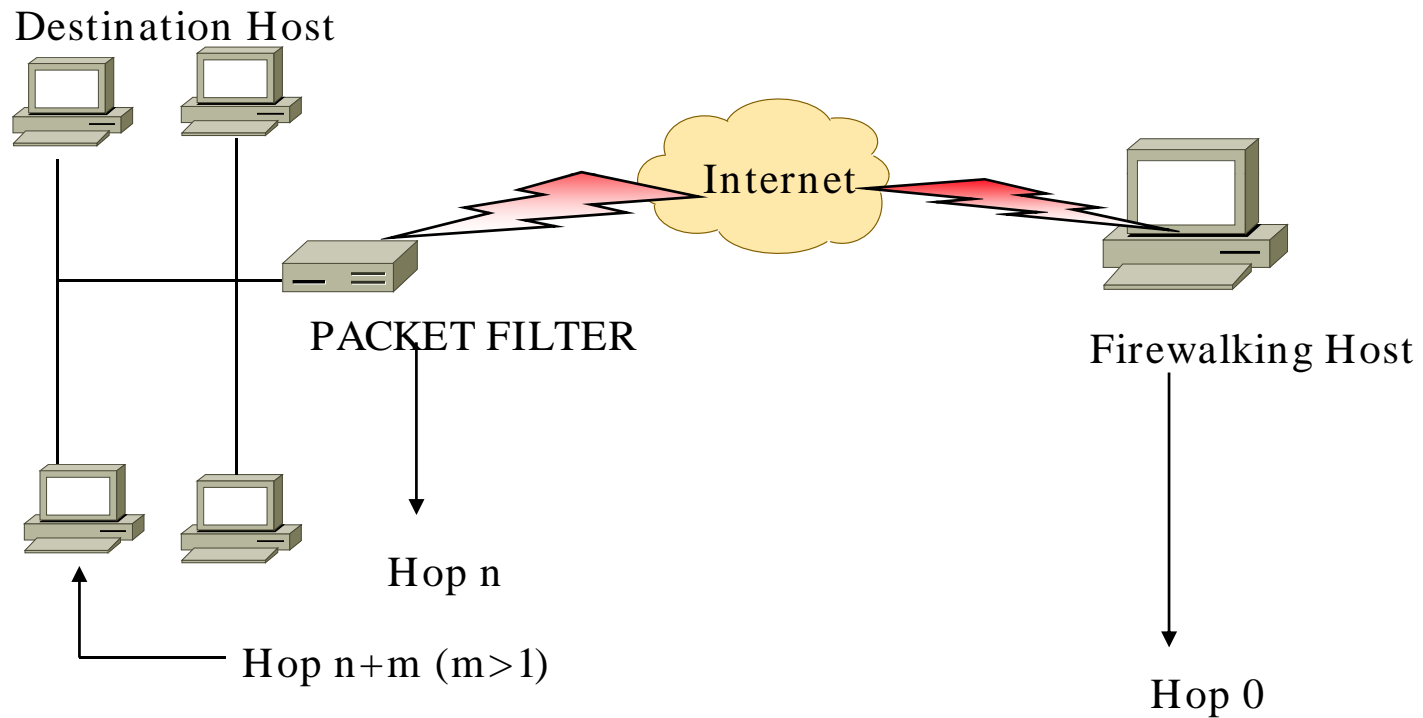
Firewalking is a tool that employs traceroute-like techniques to analyze IP packet responses to determine gateway ACL filters and map networks

The tool employs the technique to determine the filter rules in place on a packet forwarding device

Firewalk works by sending out TCP or UDP packets with a TTL one greater than the targeted gateway

- If the gateway allows the traffic, it will forward the packets to the next hop where they will expire and elicit an `ICMP_TIME_EXCEEDED` message
- If the gateway host does not allow the traffic, it will likely drop the packets on the floor and there will be no response

# Firewalk Tool (cont'd)





# Firewalk Commands

```
haja: ~# ./firewalk
Firewalk 5.0 [gateway ACL scanner]
Usage : ./firewalk [options] target_gateway metric
[-d 0 - 65535] destination port (ramping phase)
[-h] program help
[-i device] interface
[-n] do not resolve IP addresses into hostnames
[-p TCP | UDP] firewalk protocol
[-r] strict RFC adherence
[-S x - y, z] port range to scan
[-s 0 - 65535] source port
[-T 1 - 1000] packet read timeout in ms
[-t 1 - 25] IP time to live
[-v] program version
[-x 1 - 8] expire vector
```



# Firewalk Output

```
haja: ~# ./firewalk -n -s20-25, 80 172.71.234.82 172.71.254.20
Firewalk 5.0 [gateway ACL scanner]
Firewalk state initialization completed successfully.
TCP-based scan.
Ramping phase source port: 53, destination port: 33434
Hotfoot through 172.71.234.82 using 172.71.254.20 as a metric.
Ramping Phase:
 1 (TTL 1): expired [10.20.19.1]
 2 (TTL 2): expired [10.20.44.1]
 3 (TTL 3): expired [10.30.0.10]
 4 (TTL 4): expired [10.33.9.9]
 5 (TTL 5): expired [10.161.124.53]
 6 (TTL 6): expired [10.228.44.49]
 7 (TTL 7): expired [10.232.3.137]
 8 (TTL 8): expired [20.181.1.133]
 9 (TTL 9): expired [192.168.14.162]
10 (TTL 10): expired [192.168.14.121]
11 (TTL 11): expired [192.168.5.99]
12 (TTL 12): expired [192.168.5.123]
13 (TTL 13): expired [192.168.5.113]
14 (TTL 14): expired [192.168.30.14]
15 (TTL 15): expired [192.168.30.142]
16 (TTL 16): expired [172.54.229.229]
17 (TTL 17): expired [172.54.228.129]
18 (TTL 18): expired [172.54.230.254]
19 (TTL 19): expired [172.54.230.121]
20 (TTL 20): expired [172.54.230.118]
21 (TTL 21): expired [172.54.230.158]
22 (TTL 22): expired [172.54.119.229]
23 (TTL 23): expired [172.71.200.230]
24 (TTL 24): expired [172.71.234.158]
25 (TTL 25): expired [172.71.234.82]
Binding host reached.
Scan bound at 26 hops.
Scanning Phase:
port 20: A! open (port not listen) [172.71.254.20]
port 21: A! open (port not listen) [172.71.254.20]
port 22: A! open (port listen) [172.71.254.20]
port 23: A! open (port not listen) [172.71.254.20]
port 24: A! open (port not listen) [172.71.254.20]
port 25: A! open (port listen) [172.71.254.20]
port 80: A! open (port listen) [172.71.254.20]

Scan completed successfully.

Total packets sent:          32
Total packet errors:         0
Total packets caught        64
Total packets caught of interest 30
Total ports scanned         7
Total ports open:           7
Total ports unknown:        0
```

Firewalk penetrated all of the filters through the target gateway but also port scan the metric and determine the following ports open:

port 23 (telnet)

port 25 (SMTP)

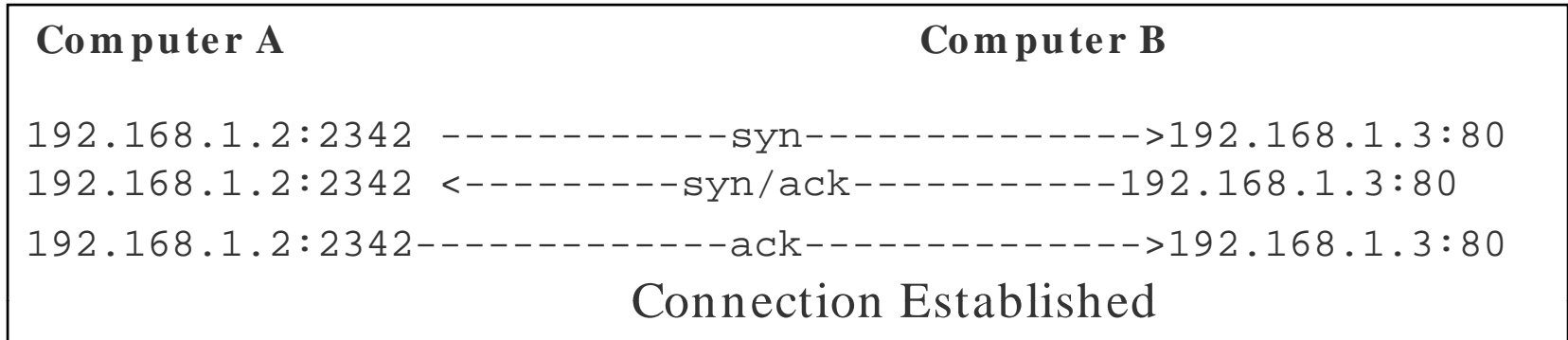
port 80 (HTTP)





# Checking for Open Ports

# Three Way Handshake



The Computer A ( 192.168.1.2 ) initiates a connection to the server ( 192.168.1.3 ) via a packet with only the **SYN** flag set

The server replies with a packet with both the **SYN** and the **ACK** flag set

For the final step, the client responds back to the server with a single **ACK** packet

If these three steps are completed without complication, then a TCP connection has been established between the client and the server

# Three Way Handshake: Screenshot

The screenshot displays a network capture in Wireshark. The packet list shows the following sequence:

No.	Source	SP	Destination	DP	Protocol	Info
1	192.168.2.4	3006	62.243.72.50	21	TCP	3006 > 21 [SYN] Seq=1664882716 Ack=0 win=16384 Len=
2	62.243.72.50	21	192.168.2.4	3006	TCP	21 > 3006 [SYN, ACK] Seq=829007135 Ack=1664882717 W
3	192.168.2.4	3006	62.243.72.50	21	TCP	3006 > 21 [ACK] Seq=1664882717 Ack=829007136 win=17
4	62.243.72.50	21	192.168.2.4	3006	FTP	Response: 220-ftp.FreeBSD.org NcFTPd server (licens
5	192.168.2.4	3006	62.243.72.50	21	TCP	3006 > 21 [ACK] Seq=1664882717 Ack=829007194 win=17
6	62.243.72.50	21	192.168.2.4	3006	FTP	Response: 220-The FreeBSD mirror at TDC, in Aarhus,
7	192.168.2.4	3006	62.243.72.50	21	TCP	3006 > 21 [ACK] Seq=1664882717 Ack=829008140 win=16
8	192.168.2.4	3006	62.243.72.50	21	FTP	Request: USER none
9	62.243.72.50	21	192.168.2.4	3006	FTP	Response: 421 only anonymous logins are allowed her
10	192.168.2.4	3006	62.243.72.50	21	TCP	3006 > 21 [ACK] Seq=1664882728 Ack=829008185 win=16
11	192.168.2.4	3006	62.243.72.50	21	FTP	Request: QUIT

The packet details pane shows the selected SYN-ACK packet (No. 2):

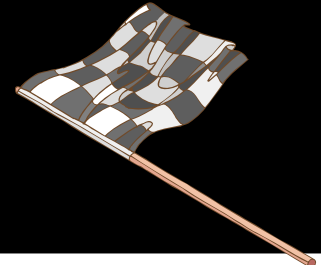
- Transmission Control Protocol, Src Port: 21 (21), Dst Port: 3006 (3006), Seq: 829007135, Ack: 1664882717
- source port: 21 (21)
- Destination port: 3006 (3006)
- Sequence number: 829007135
- Acknowledgement number: 1664882717**
- Header length: 24 bytes

The raw packet bytes pane shows the following hex and ASCII data:

```

0000 00 04 76 47 20 1b 00 a0 c5 59 47 d4 08 00 45 00  ..VG ... .YG...E.
0010 00 2c 9b 17 40 00 2a 06 6b e3 3e f3 48 32 c0 a8  ....@.*. k.>.H2..
0020 02 04 00 15 0b be 31 69 a5 1f 53 3c 18 16 60 12  .....1f ..C<.. .
0030 e0 00 10 8f 00 00 02 04 05 b4 00 00  ..
  
```

The filter bar at the bottom shows the filter: Acknowledgement number (tcp.ack), 4 bytes.



Standard TCP communications are controlled by flags in the TCP packet header

The flags are as follows:

- **Synchronize** – It is also called as "SYN" and is used to initiate a connection between hosts
- **Acknowledgement** - It is also called as "ACK" and is used in establishing a connection between hosts
- **Push** – It is called as "PSH" and instructs receiving system to send all buffered data immediately
- **Urgent** - It is also called as "URG" and states that the data contained in the packet should be processed immediately
- **Finish** – It is also called as "FIN" and tells remote system that there will be no more transmissions
- **Reset** – It is also called "RST" and is used to reset a connection

Nmap is a free open source utility for network exploration

It is designed to rapidly scan large networks

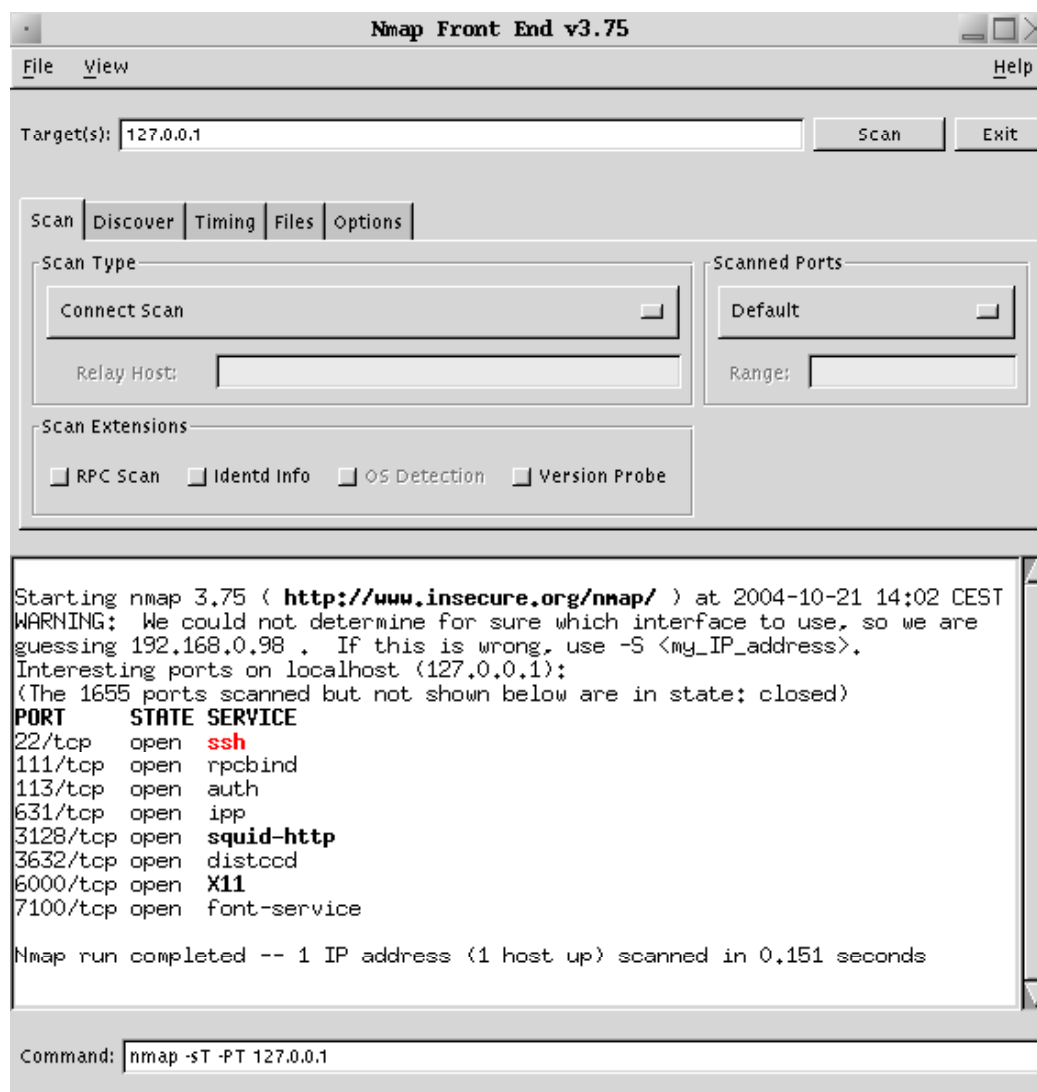
### Features:

- Nmap is used to carry out port scanning, OS detection, version detection, ping sweep, and many other techniques
- It scans a large number of machines at one time
- It is supported by many operating systems
- It can carry out all types of port scanning techniques





# Nmap: Screenshot



# Nmap: Scan Methods

Some of the scan methods used by Nmap:

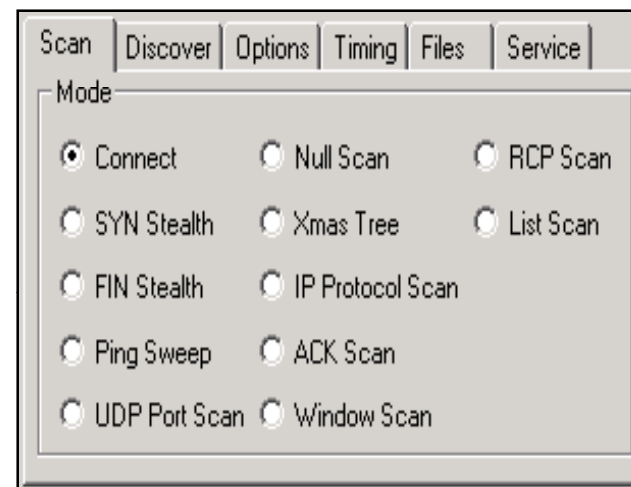
**Xmas Tree:** The attacker checks for TCP services by sending "Xmas-tree" packets

**SYN Stealth:** It is referred to as "half-open" scanning, as full TCP connection is not opened

**Null Scan:** It is an advanced scan that may be able to pass through unmolested firewalls

**Windows Scan:** It is similar to the ACK scan and can also detect open ports

**ACK Scan:** It is used to map out firewall ruleset



# Nmap: Scan Methods

Nmap Scan	Command Syntax	Requires Privileged Access	Identifies TCP Ports	Identifies UDP Ports
TCP SYN Scan	-sS	YES	YES	NO
TCP connect() Scan	-sT	NO	YES	NO
FIN Scan	-sF	YES	YES	NO
Xmas Tree Scan	-sX	YES	YES	NO
Null Scan	-sN	YES	YES	NO
Ping Scan	-sP	NO	NO	NO
Version Detection	-sV	NO	NO	NO
UDP Scan	-sU	YES	NO	YES
IP Protocol Scan	-sO	YES	NO	NO
ACK Scan	-sA	YES	YES	NO
Window Scan	-sW	YES	YES	NO
RPC Scan	-sR	NO	NO	NO
List Scan	-sL	NO	NO	NO
Idlescan	-sI	YES	YES	NO
FTP Bounce Attack	-b	NO	YES	NO

# NMAP Scan Options

**-sT** (TcpConnect)

**-sS** (SYN scan)

**-sF** (Fin Scan)

**-sX** (Xmas Scan)

**-sN** (Null Scan)

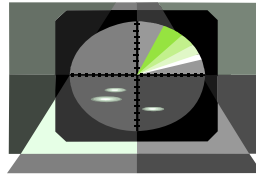
**-sP** (Ping Scan)

**-sU** (UDP scans)

**-sO** (Protocol Scan)

**-sI** (Idle Scan)

**-sA** (Ack Scan)



**-sW** (Window Scan)

**-sR** (RPC scan)

**-sL** (List/Dns Scan)

**-P0** (don't ping)

**-PT** (TCP ping)

**-PS** (SYN ping)

**-PI** (ICMP ping)

**-PB** (= PT + PI)

**-PP** (ICMP timestamp)

**-PM** (ICMP netmask)

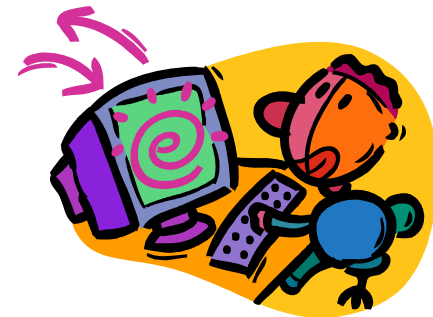
# NMAP Output Format

**-oN**(ormal)

**-oX**(ml)

**-oG**(repable)

**-oA**(ll)



# NMAP Timing Options

**-T Paranoid** – serial scan & 300 sec wait

**-T Sneaky** - serialize scans & 15 sec wait

**-T Polite** - serialize scans & 0.4 sec wait

**-T Normal** – parallel scan

**-T Aggressive**- parallel scan & 300 sec timeout & 1.25 sec/probe

**-T Insane** - parallel scan & 75 sec timeout & 0.3 sec/probe

**--host\_timeout --max\_rtt\_timeout**  
(default - 9000)

**--min\_rtt\_timeout --initial\_rtt\_timeout**  
(default – 6000)

**--max\_parallelism --scan\_delay** (between probes)



# NMAP Options

`--resume` (scan) `--append_output`

`-iL` <targets\_filename> `-p` <port ranges>

`-F` (Fast scan mode) `-D` <decoy1 [,decoy2][,ME],>

`-S` <SRC\_IP\_Address> `-e` <interface>

`-g` <portnumber> `--data_length` <number>

`--randomize_hosts` `-O` (OS fingerprinting) `-I` (dent-scan)

`-f` (fragmentation) `-v` (verbose) `-h` (help)

`-n` (no reverse lookup) `-R` (do reverse lookup)

`-r` (don't randomize port scan) `-b` <ftp relay host> (FTP bounce)



HPING is a command-line oriented TCP/IP packet assembler/ analyzer

It has a Traceroute mode

It has the ability to send files between a covered channel

It not only sends but also supports ICMP echo requests

- TCP
- UDP
- ICMP and
- Raw-IP protocols

### Features

- Firewall testing
- Advanced port scanning
- Network testing, using different protocols, TOS, fragmentation
- Advanced Traceroute, under all the supported protocols
- Remote OS fingerprinting
- Remote uptime guessing
- TCP/IP stacks auditing

# Hping2 Commands

**hping2 10.0.0.5**

- This command sends a TCP null-flags packet to port 0 of host 10.0.0.5

**hping2 10.0.0.5 -p 80**

- This command sends the packet to port 80

**hping2 -a 10.0.0.5 -s -p 81 10.0.0.25**

- This command sends spoofed SYN packets to the target via a trusted third party to port 81

**hping www.debian.org -p 80 -A**

- This command sends ACK to port 80 of www.debian.org

**hping www.yahoo.com -p 80 -A**

- This command checks for IPID responses

```

C:\WINDOWS\System32\cmd.exe
J:\Ethical Hacking and Countermeasures v5\Module 03 - Scanning\Hping2 for Windo
s>hping2 --help
usage: hping host [options]
-h --help          show this help
-v --version       show version
-c --count         packet count
-i --interval     wait <uX> for X microseconds, for example -i u1000
-f --fast         alias for -i u10000 (10 packets for second)
-n --numeric      numeric output
-q --quiet        quiet
-I --interface    interface name (otherwise default routing interface)
-U --verbose      verbose mode
-D --debug        debugging info
-z --bind         bind ctrl+z to ttl (default to dst port)
-Z --unbind      unbind ctrl+z
Mode
default mode     TCP
-0 --rawip       RAW IP mode
-1 --icmp        ICMP mode
-2 --udp         UDP mode
-? --listen      listen mode
IP
-a --spoo        spoof source address
--rand-dest      random destination address mode. see the man.
--rand-source    random source address mode. see the man.
-t --ttl         ttl (default 64)
-M --id         id (default random)
-W --winid       use wins id byte ordering
-r --rel         relativize id field (to estimate host traffic)
-f --frag        split packets in more frag. (may pass weak acl)
-x --morefrag    set more fragments flag
-y --dontfrag    set dont fragment flag
-g --fragoff     set the fragment offset
-m --mtu         set virtual mtu, implies --frag if packet size > mtu
-o --tos         type of service (default 0x00). try --tos help
-C --rout        includes RECORD_ROUTE option and display the route buffer
-lsrr           loose source routing and record route
--csrr          strict source routing and record route
-H --ipproto     set the IP protocol field, only in RAW IP mode
ICMP
-C --icmptype    icmp type (default echo request)
-K --icmpcode    icmp code (default 0)
--icmp-ts        Alias for --icmp --icmptype 13 (ICMP timestamp)
--icmp-addr      Alias for --icmp --icmptype 17 (ICMP address subnet mask)
--icmp-help      display help for others icmp options
UDP/TCP
-s --baseport    base source port (default random)
-p --dstport     [!+!+Kport] destination port(default 0) ctrl+z inc/dec
-k --keep        keep still source port
-w --win         winsize (default 64)
-o --tcpoff      set fake tcp data offset (instead of tcphdrLen / 4)
-Q --seqnum      shows only tcp sequence number
-h --badcksum    (try to) send packets with a bad IP checksum
many systems will fix the IP checksum sending the packet
so you'll get bad UDP/TCP checksum instead.
-M --setseq      set TCP sequence number
-L --setack      set TCP ack
-F --fin         set FIN flag
-S --syn         set SYN flag
-T --rst         set RST flag
-P --push        set PUSH flag
-A --ack         set ACK flag
-U --urg         set URG flag
-X --xmas        set X unused flag (0x40)
-Y --ymas        set Y unused flag (0x80)
--tcpexitcode   use last tcp->th_flags as exit code
--tcp-timestamp enable the TCP timestamp option to guess the HZ/uptime
Common
-d --data        data size (default is 0)
-E --file        data from file
-e --sign        add 'signature'
-i --dump        dump packets in hex
-I --print       dump printable characters
  
```

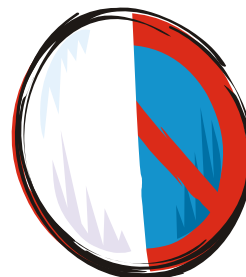
# SYN Stealth / Half Open Scan

SYN Stealth / Half Open Scan is often referred to as half open scan because it does not open a full TCP connection

First, a SYN packet is sent to a port of the machine, suggesting a request for connection, and the response is awaited

If the port sends back a SYN/ ACK packet, then it is inferred that a service at the particular port is listening. If an RST is received, then the port is not active/ listening. As soon as the SYN/ ACK packet is received, an RST packet is sent, instead of an ACK, to tear down the connection

The key advantage is that fewer sites log this scan

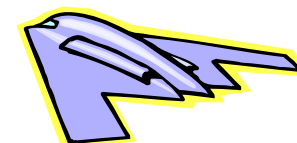


# Stealth Scan

Computer A

Computer B

```
192.168.1.2:2342 -----syn-----  
>192.168.1.3:80  
192.168.1.2:2342 <-----syn/ack-----  
192.168.1.3:80  
192.168.1.2:2342-----RST-----  
>192.168.1.3:80
```



Client sends a single **SYN** packet to the server on the appropriate port

If the port is open then the server responds with a **SYN/ACK** packet

If the server responds with an **RST** packet, then the remote port is in "closed" state

The client sends the **RST** packet to close the initiation before a connection can ever be established

This scan is also known as "half-open" scan



## Computer A

## Computer B

### Xmas scan directed at open port:

```
192.5.5.92:4031 -----FIN/URG/PSH----->192.5.5.110:23  
192.5.5.92:4031 <-----NO RESPONSE-----192.5.5.110:23
```

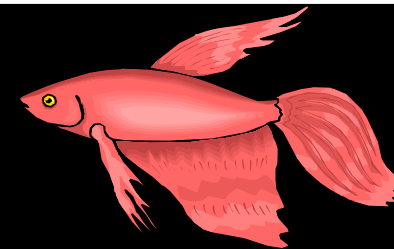
### Xmas scan directed at closed port:

```
192.5.5.92:4031 -----FIN/URG/PSH----->192.5.5.110:23  
192.5.5.92:4031<-----RST/ACK-----192.5.5.110:23
```

Note: XMAS scan only works if OS system's TCP/IP implementation is developed according to RFC 793

Xmas Scan will not work against any current version of Microsoft Windows

Xmas scans directed at any Microsoft system will show all ports on the host as being closed



**Computer A**

**Computer B**

**FIN scan directed at open port:**

```
192.5.5.92:4031 -----FIN----->192.5.5.110:23  
192.5.5.92:4031 <-----NO RESPONSE-----192.5.5.110:23
```

**FIN scan directed at closed port:**

```
192.5.5.92:4031 -----FIN-----192.5.5.110:23  
192.5.5.92:4031<-----RST/ACK-----192.5.5.110:23
```

Note: FIN scan only works if OS' TCP/IP implementation is developed according to RFC 793

FIN Scan will not work against any current version of Microsoft Windows

FIN scans directed at any Microsoft system will show all ports on the host as being closed



## Computer A

## Computer B

### NULL scan directed at open port:

```
192.5.5.92:4031 -----NO FLAGS SET----->192.5.5.110:23  
192.5.5.92:4031 <-----NO RESPONSE-----192.5.5.110:23
```

### NULL scan directed at closed port:

```
192.5.5.92:4031 -----NO FLAGS SET-----192.5.5.110:23  
192.5.5.92:4031<-----RST/ACK-----192.5.5.110:23
```

Note: NULL scan only works if OS' TCP/IP implementation is developed according to RFC 793

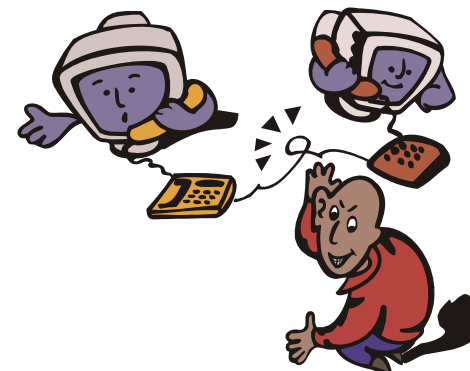
NULL Scan will not work against any current version of Microsoft Windows

NULL scans directed at any Microsoft system will show all ports on the host as being closed

Almost four years ago, security researcher Antirez posted an innovative new TCP port scanning technique

IDLE Scan, as it has become known, allows for completely blind port scanning

Attackers can actually scan a target without sending a single packet to the target from their own IP address





# IDLE Scan: Basics

Most network servers listen on TCP ports, such as web servers on port 80 and mail servers on port 25

A port is considered "open" if an application is listening on the port, otherwise it is closed

One way to determine whether a port is open is to send a "SYN" (session establishment) packet to the port

The target machine will send back a "SYN|ACK" (session request acknowledgment) packet if the port is open, and an "RST" (Reset) packet if the port is closed

A machine which receives an unsolicited SYN|ACK packet will respond with an RST. An unsolicited RST will be ignored

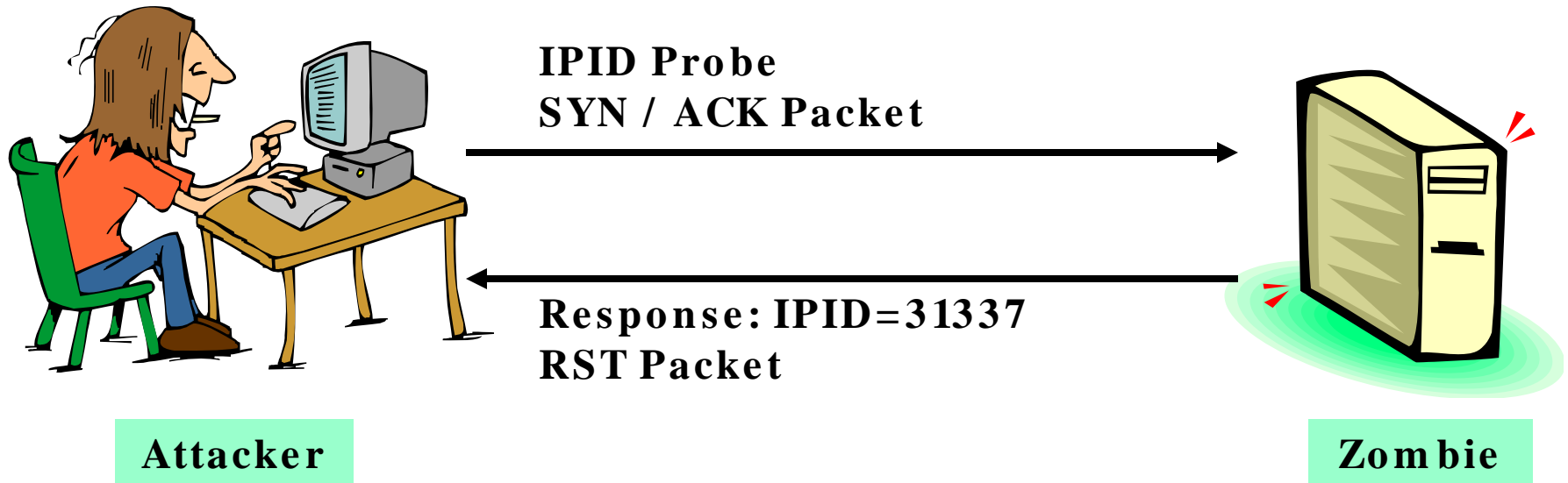
Every IP packet on the Internet has a "fragment identification" number

Many operating systems simply increment this number for every packet they send

So probing for this number can tell an attacker how many packets have been sent since the last probe

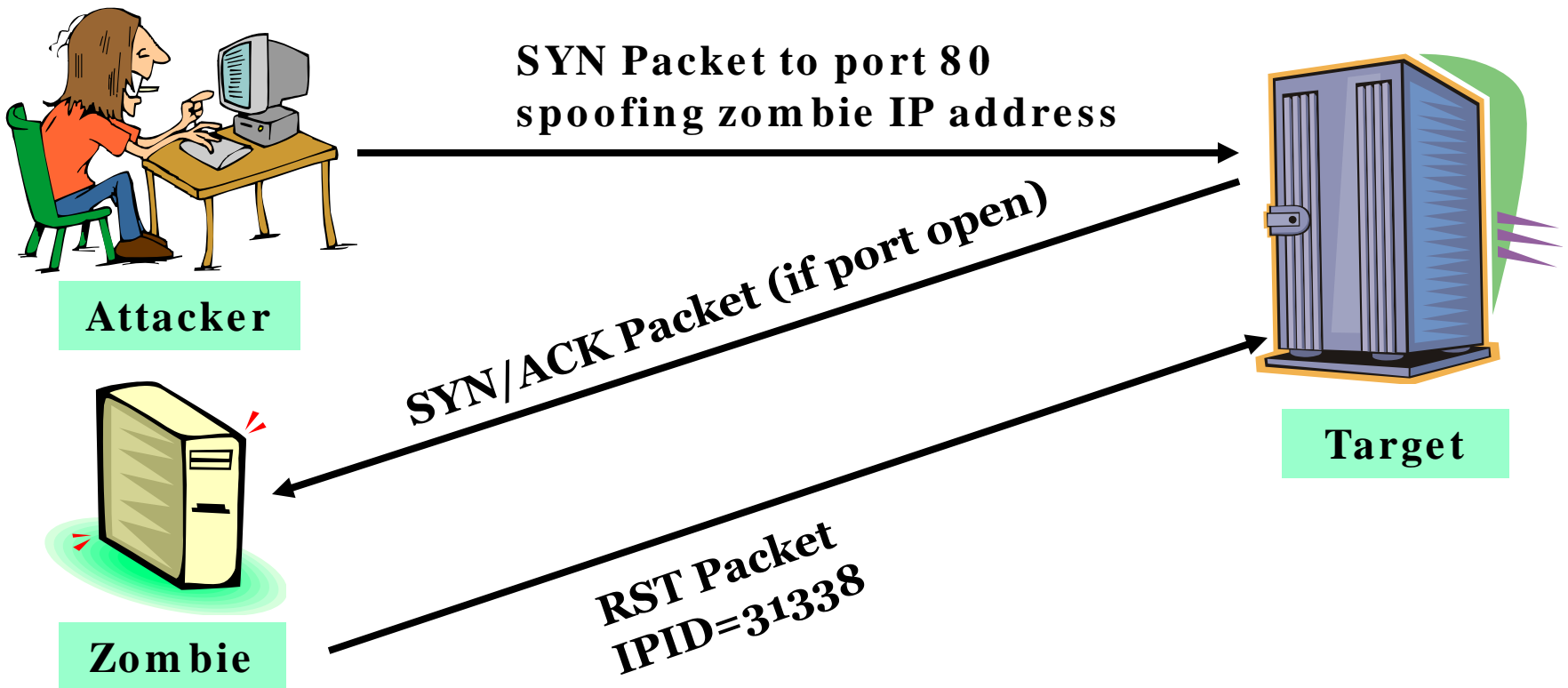
# IDLE Scan: Step 1

Choose a "zombie" and probe for its current IPID number



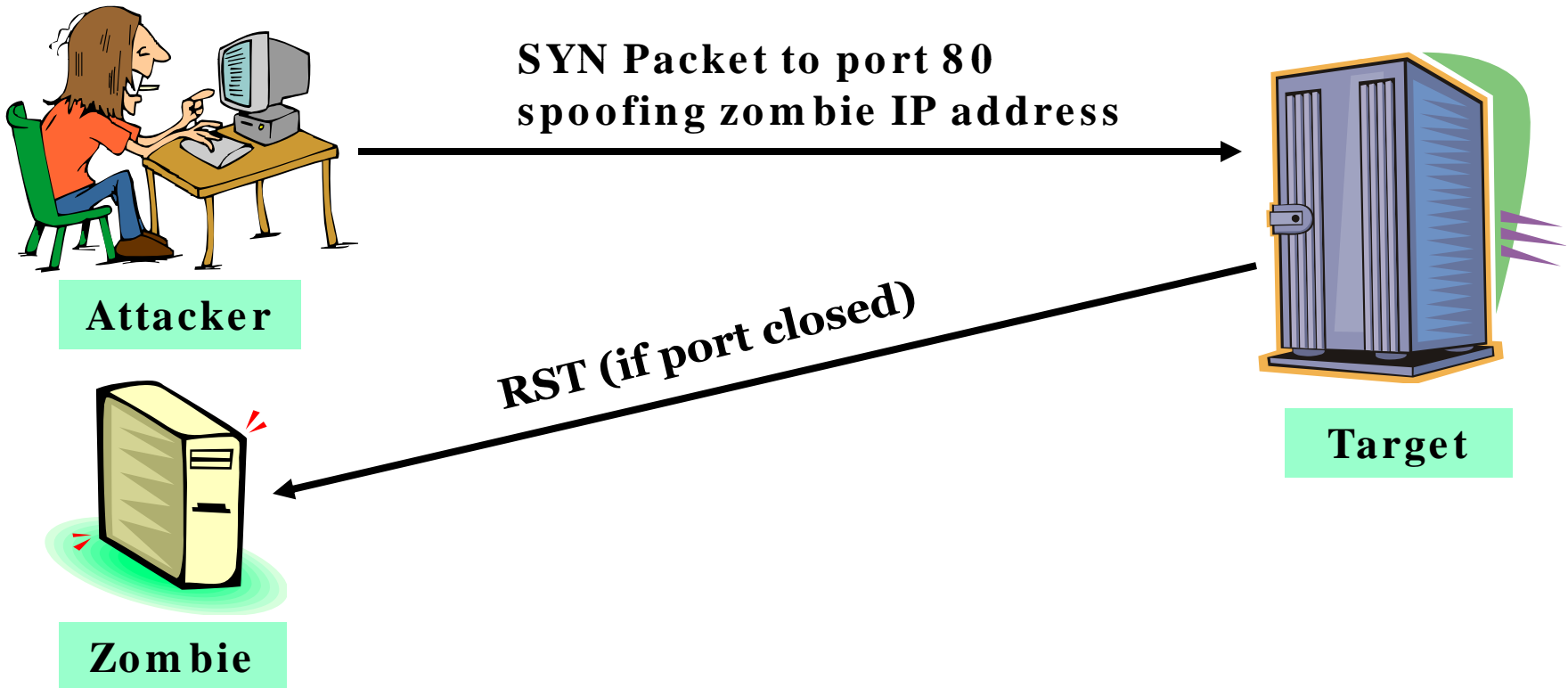
# IDLE Scan: Step 2.1 (Open Port)

Send SYN packet to target machine spoofing the IP address of the “zombie”



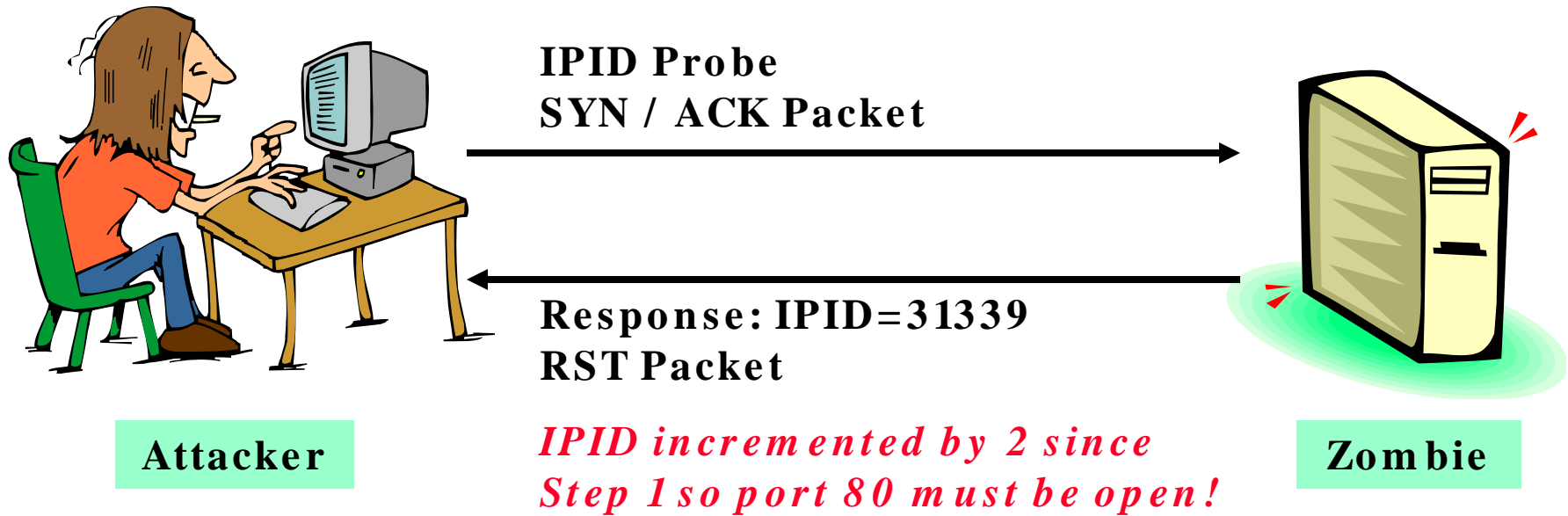
# IDLE Scan: Step 2.2 (Closed Port)

The target will send RST to the “zombie” if port is closed. Zombie will not send anything back



# IDLE Scan: Step 3

Probe "zombie" IPID again



# ICMP Echo Scanning/List Scan

## ICMP Echo Scanning

- This is not really port scanning, since ICMP does not have a port abstraction
- But it is sometimes useful to determine which hosts in a network are up by pinging them all
- `nmap -P cert.org/24 152.148.0.0/16`



## List Scan

- This type of scan simply generates and prints a list of IPs/Names without actually pinging or port scanning them
- A DNS name resolution will also be carried out



# TCP Connect / Full Open Scan

This is the most reliable form of TCP scanning

The `connect()` system call provided by the operating system is used to open a connection to every open port on the machine

If the port is open, `connect()` will succeed

If the port is closed, then it is unreachable



ACK

SYN

ACK

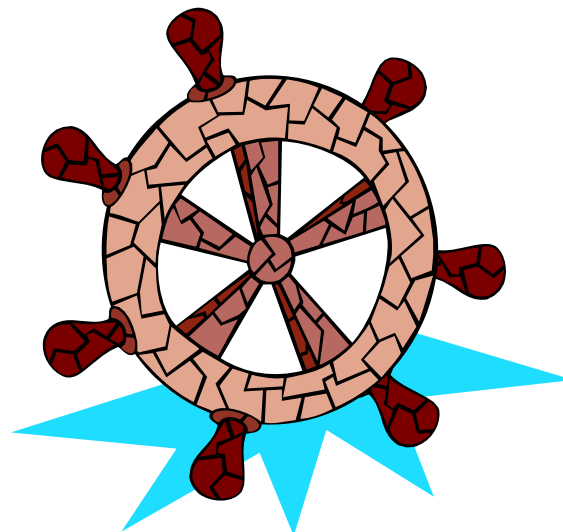
SYN

+  
ACK

# SYN/FIN Scanning Using IP Fragments

It is not a new scanning method but a modification of the earlier methods

The TCP header is split up into several packets so that the packet filters are not able to detect what the packets intend to do





# UDP Scanning

## UDP RAW ICMP Port Unreachable Scanning

- This scanning method uses a UDP protocol instead of a TCP protocol
- Though this protocol is simpler, scanning it is more difficult

## UDP RECVFROM() Scanning

- While non root users cannot read port unreachable errors directly, LINUX is intuitive enough to inform the users indirectly when they have been received
- This is the technique used for determining open ports by non root users



# Reverse Ident Scanning

The Ident protocol allows for the disclosure of the username of the owner of any process connected via TCP, even if that process did not initiate the connection

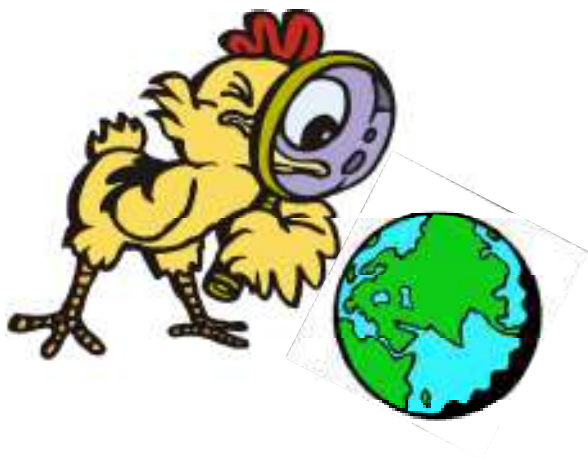
So a connection can be established with the http port and then use Ident to find out whether the server is running as a root

This can be done only with a full TCP connection to the target port



# Window Scan

This scan is similar to the ACK scan, except that it can sometimes detect open ports as well as filtered/unfiltered ports due to an anomaly in the TCP window size reported by some operating systems



# Blaster Scan

A TCP port scanner for UNIX-based operating systems

Ping target hosts for examining connectivity

Scans subnets on a network

Examines FTP for anonymous access

Examines CGI bugs

Examines POP3 and FTP for brute force vulnerabilities



# PortScan Plus, Strobe

## PortScan Plus

- Windows-based scanner developed by Peter Harrison
- The user can specify a range of IP addresses and ports to be scanned
- When scanning a host or a range of hosts, it displays the open ports on those hosts

## Strobe

- A TCP port scanner developed by Julian Assange
- Written in C for UNIX-based operating systems
- Scans all open ports on the target host
- Provides only limited information about the host



```
C:\WINNT\System32\cmd.exe
ipEye 1.2 - (c) 2000-2001, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
          - http://ntsecurity.nu/toolbox/ipeye/

Error: Too few parameters.

Usage:

ipEye <target IP> <scantype> -p <port> [optional parameters]
ipEye <target IP> <scantype> -p <from port> <to port> [optional parameters]

<scantype> is one of the following:
  -syn  = SYN scan
  -fin  = FIN scan
  -null = Null scan
  -xmas = Xmas scan

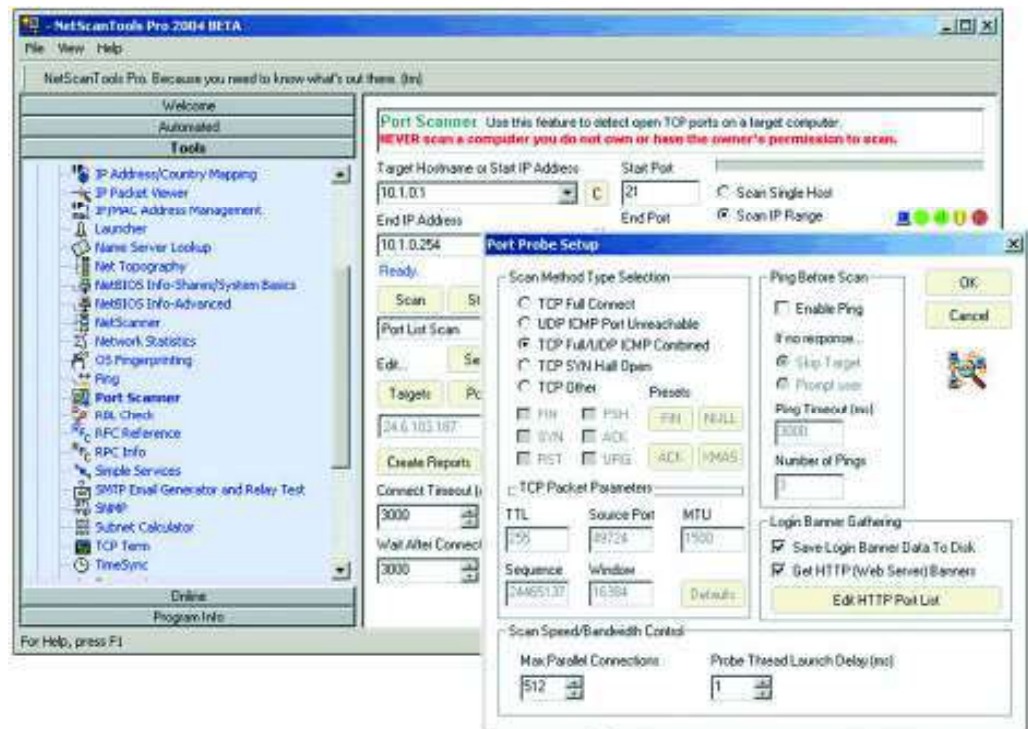
(note: FIN, Null and Xmas scans don't work against Windows systems.)

[optional parameters] are selected from the following:
  -sip <source IP> = source IP for the scan
  -sp  <source port> = source port for the scan
  -d  <delay in ms> = delay between scanned ports in milliseconds
                    (default set to 750 ms)
```

IPSecScan is a tool that can scan either a single IP address or a range of IP addresses looking for systems that are IPSec-enabled

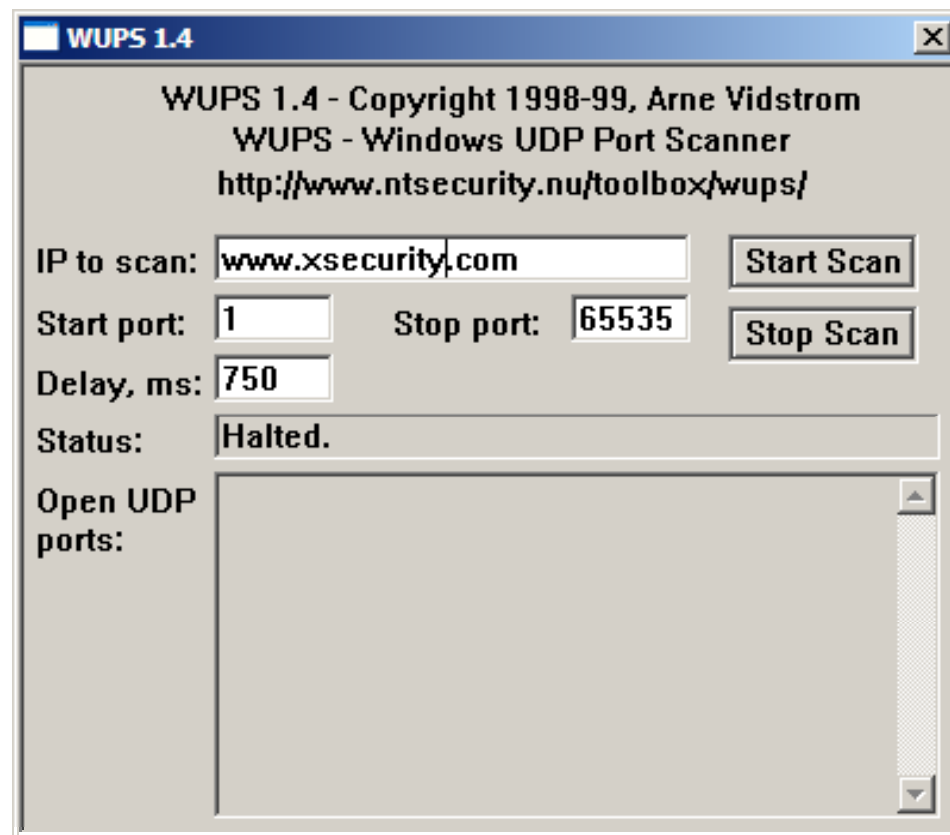
It is used to:

- Determine the ownership of IP addresses
- Translate IP addresses to hostnames
- Scan networks
- Probe ports of target computers for services
- Validate email addresses
- Determine the ownership of domains
- List the computers in a domain

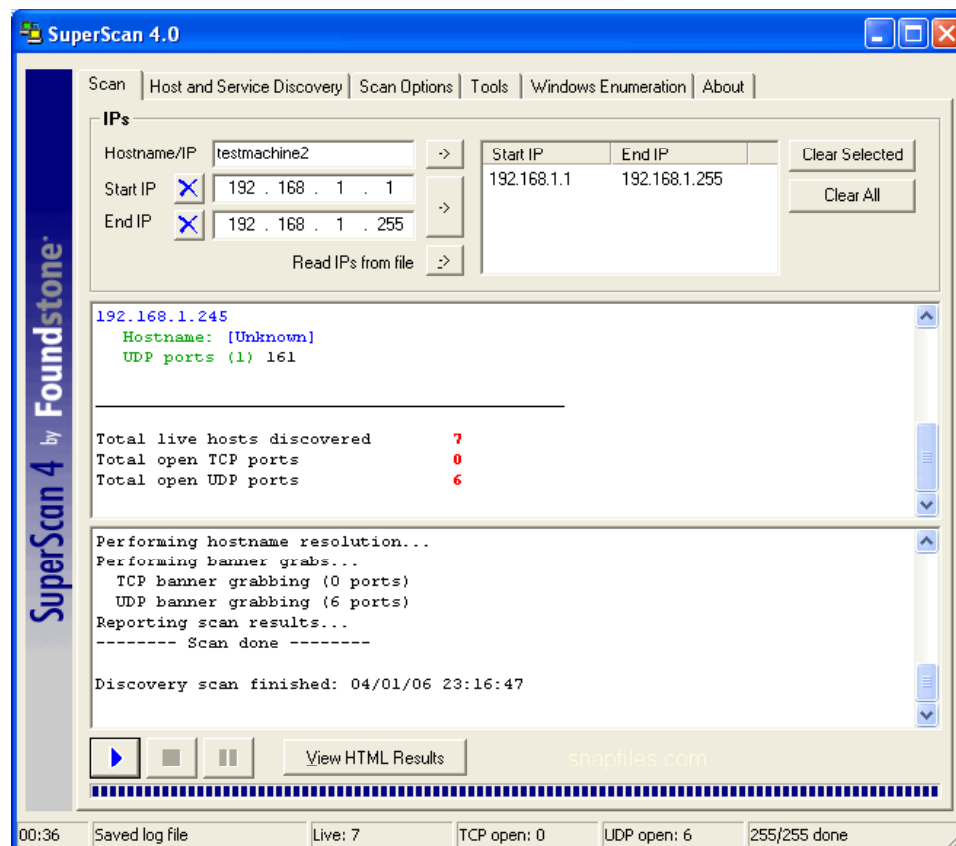


# WUPS – UDP Scanner

WUPS is a simple but effective UDP scanner for Windows with a graphical interface







It is a TCP port scanner, pinger, and hostname resolver

It can perform ping scans, scans port using any IP range, and scans any port range from a built-in list or specified range

IPScanner performs different types of scans on each target IP address and reports the results in a nice graphical format for your review

The scan types are :

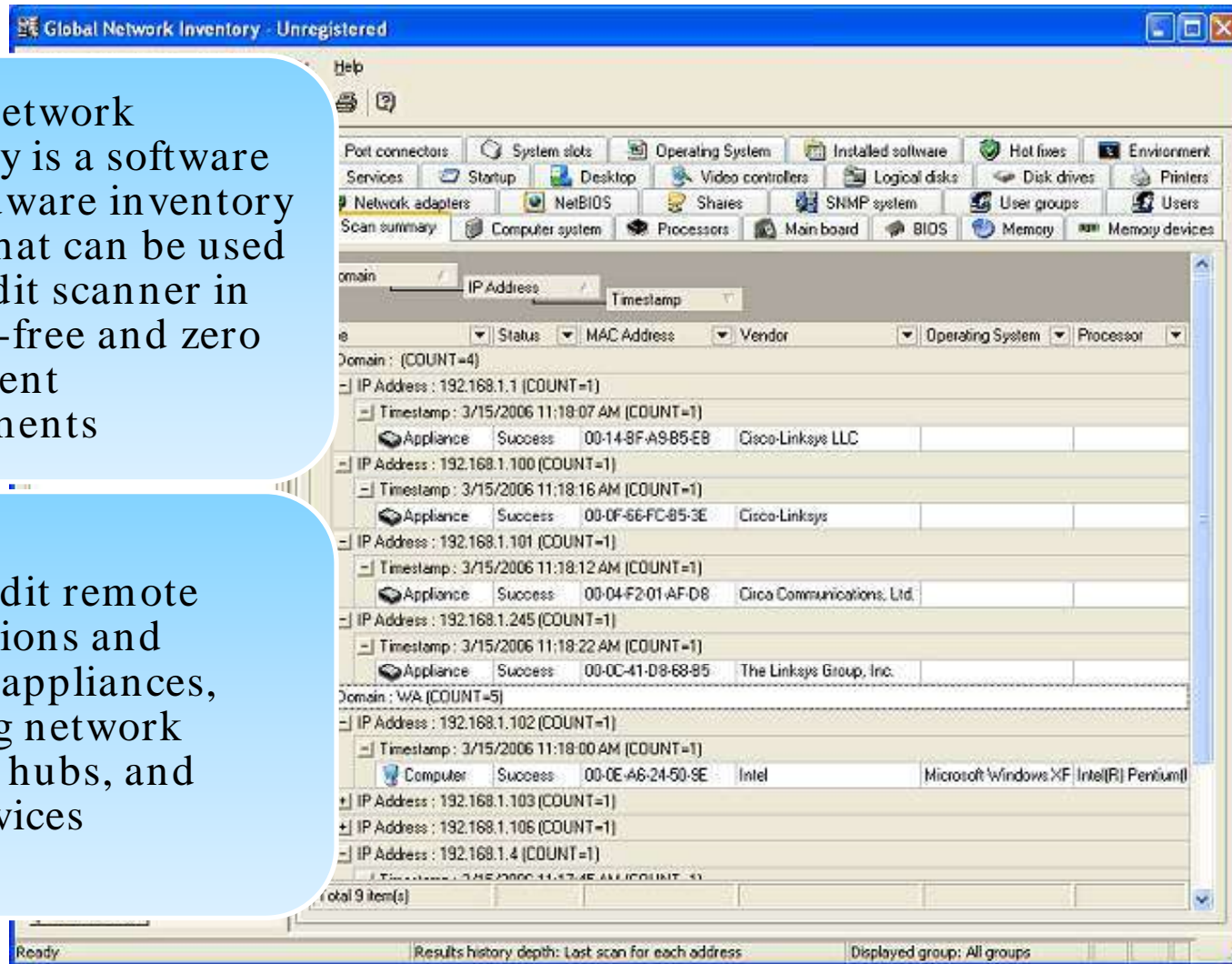
- Pingscan
- TCP Port scan
- Netbios scan
- NT Services scan
- Local Groups scan
- Remote Time of Day scan



# Global Network Inventory Scanner

Global Network Inventory is a software and hardware inventory system that can be used as an audit scanner in an agent-free and zero deployment environments

It can audit remote workstations and network appliances, including network printers, hubs, and other devices



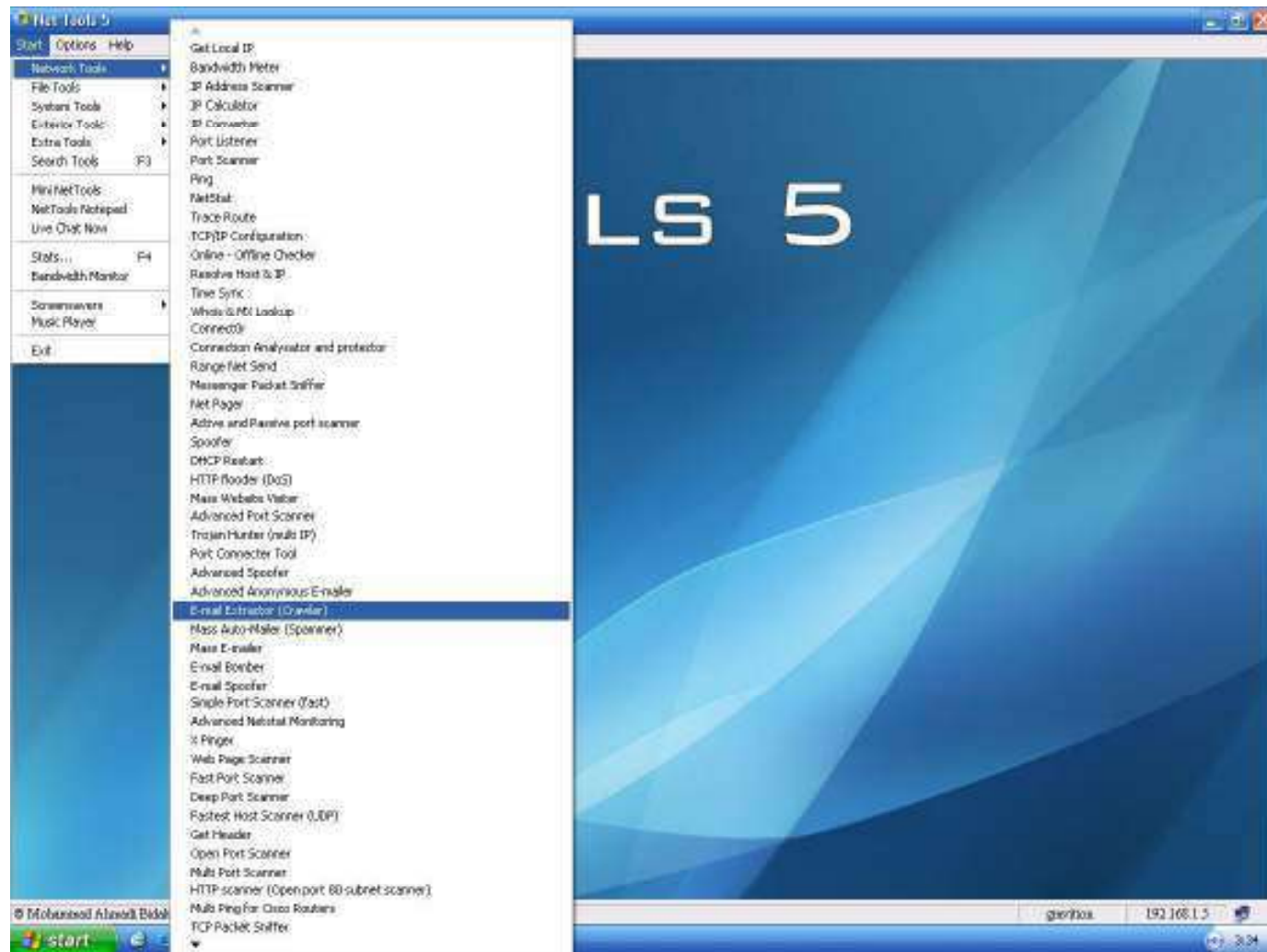
# Net Tools Suite Pack

Net Tools Suite Pack is a collection of scanning tools

This toolset contains tons of port scanners, flooders, web rippers, and mass e-mailers



# Net Tools Suite Pack: Screenshot



# FloppyScan

Floppyscan is a dangerous hacking tool which can be used to portscan a system using a floppy disk

It boots up mini Linux

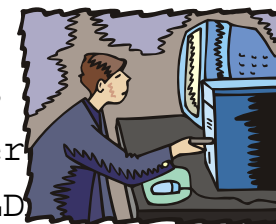
It displays “Blue screen of death” screen

It port scans the network using NMAP

It sends the results by e-mail to a remote server

Interesting ports on 192.168.100.5:  
(The 1646 ports scanned but not shown below are in state: closed)

PORT	STATE	SERVICE
53/tcp	open	domain
88/tcp	open	kerberos-sec
135/tcp	open	msrpc
139/tcp	open	netbios-ss
389/tcp	open	ldap
445/tcp	open	microsoft-ds
464/tcp	open	kpasswd5
593/tcp	open	http-rpc-epmap
636/tcp	open	ldapssl
1025/tcp	open	NFS-or-IIS
1026/tcp	open	LSA-or-nter
3268/tcp	open	globalcatLD
3269/tcp	open	globalcatLDAPssl





# FloppyScan Steps



**Step1:** Walk to a PC and insert the Floppy scan disk and restart the machine



**Step2:** The system boots to floppy and BSOD is displayed on the screen



**Step3:** Performs NMAP scan on the local network



**Step4:** Sends the results through e-mail

# E-mail Results of FloppyScan

```
nameserver 192.168.100.5
# nmap 3.50 scan initiated Tue Oct 19 12:21:04 2004 as: nmap -sS -n
Host 192.168.100.0 seems to be a subnet broadcast address (returned
All 1659 scanned ports on 192.168.100.1 are: filtered
```

Interesting ports on 192.168.100.5:  
(The 1646 ports scanned but not shown below are in state: closed)

PORT	STATE	SERVICE
53/tcp	open	domain
88/tcp	open	kerberos-sec
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
389/tcp	open	ldap
445/tcp	open	microsoft-ds
464/tcp	open	kpasswd5
593/tcp	open	http-rpc-epmap
636/tcp	open	ldapssl
1025/tcp	open	NFS-or-IIS
1026/tcp	open	LSA-or-nterm
3268/tcp	open	globalcatLDAP
3269/tcp	open	globalcatLDAPssl

Interesting ports on 192.168.100.15:  
(The 1642 ports scanned but not shown below are in state: closed)

PORT	STATE	SERVICE
25/tcp	open	smtp
27/tcp	open	nsw-fe
110/tcp	open	pop3
119/tcp	open	nntp
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
143/tcp	open	imap
389/tcp	open	ldap
563/tcp	open	snews
593/tcp	open	http-rpc-epmap
636/tcp	open	ldapssl
993/tcp	open	imaps
995/tcp	open	pop3s
1031/tcp	open	iad2
1040/tcp	open	netsaint
1050/tcp	open	java-or-OTGfileshare
1059/tcp	open	nimreg

Interesting ports on 192.168.100.31:  
(The 1655 ports scanned but not shown below are in state: closed)

PORT	STATE	SERVICE
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
1025/tcp	open	NFS-or-IIS

Interesting ports on 192.168.100.32:  
(The 1649 ports scanned but not shown below are in state: closed)

PORT	STATE	SERVICE
25/tcp	open	smtp
80/tcp	open	http
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
443/tcp	open	https





# Atelier Web Ports Traffic Analyzer (AWPTA)

AWPTA captures the data that flows in and out of your PC since the time of booting

Atelier Web Ports Traffic Analyzer provides Real-time mapping of ports to processes (applications and services) and shows history since boot time of every TCP, UDP, or RAW port opened through Winsock

Optionally, AWPTA can also log (up to 500mb) all traffic since the last boot to a file



# Atelier Web Ports Traffic Analyzer (AWPTA): Screenshot

**AW Ports Traffic Analyser 2.01**

File Run Help

**Processes**

File	Pid	Bytes Sent	Bytes Rcvd
C:\Program Files\Weather Pulse\weatherpulse.exe	1904	50937	9742025
C:\PROGRA~1\INTERN~1\explore.exe	3632	17921	108468
C:\PROGRA~1\INTERN~1\explore.exe	2356	3539	27368
C:\PROGRA~1\NORTON~1\navapw32.exe	1712	309708	311675

Total Bytes Sent: 2028144 | Total Bytes Received: 15181774

Pause Purge Archive

**Details (weatherpulse.exe - PID: 1904)**

Protocol	Source	Destination	Bytes Sent	Bytes Rcvd	Opened
TCP (Client)	192.168.1.5:1052	63.111.24.29:80	278	55410	9/17/2003
TCP (Client)	0.0.0.0:1066	63.111.24.20:80	367	166	9/17/2003
TCP (Client)	192.168.1.5:1066	209.197.237.20:80	167	711	9/17/2003
TCP (Client)	0.0.0.0:1070	209.247.226.78:80	272	2781	9/17/2003

**Data**

S/R	Packet	Offset	Hex	ASCII
S	0x0001	0x0060	43 6F 6E 74 72 6F 6C 73-2...	Controls.co...
S	0x0001	0x0070	6F 73 74 3A 20 77 77 77-2...	ost: www.tr...
S	0x0001	0x0080	65 73 69 67 6E 73 2E 6E-6...	esigns.net...
S	0x0001	0x0090	65 2D 43 6F 6E 74 72 6F-6...	e-Control: ...
S	0x0001	0x00A0	63 68 65 0D 0A 0D 0A - ...	che.....
R	0x0002	0x0000	48 54 54 50 3F 31 2E 31-2...	HTTP/1.1 20...
R	0x0002	0x0010	0A 44 61 7A 65 3A 20 54-6...	.Date: Thu, ...
R	0x0002	0x0020	65 70 20 32 30 30 33 20-3...	ep 2003 00:...
R	0x0002	0x0030	20 47 4D 54 0D 0A 53 65-7...	GMT..Serve...

Traffic Archives

**STATUS**

- Buffer (Red light)
- Processes (Green light)
- Sockets (Green light)
- Index (Green light)

AW

Refresh (Green button)

Exit (Red button)

# Atelier Web Security Port Scanner (AWSPPS)

AWSPPS provides useful information about other networked machines and users on a local area network

It also provides traffic details for TCP and UDP traffic, as well as for control packets (ICMP), including ping

## Features:

- Provides TCP scanning functionality
- UDP Port Scanning
- Local Network Enumeration
- High-level of detail on the local network set-up



# AWSPS: Connections and Listening Ports. TCP, UDP and ICMP Statistics

**AW Security Port Scanner 4.61 Professional**

File Run Utilities Help

**High-Power Network Tools** for all 32-bit Windows platforms

Ports Routing IP/Transport Protocols Interfaces Registry LAN Refresh Auto 2 sec.

**LOCAL**

**Connections and Listening Ports:**

Proto	Local Address	Remote Address	State
TCP	0.0.0.0:7	0.0.0.0:0	lister
TCP	0.0.0.0:9	0.0.0.0:0	lister
TCP	0.0.0.0:13	0.0.0.0:0	lister
TCP	0.0.0.0:17	0.0.0.0:0	lister
TCP	0.0.0.0:19	0.0.0.0:0	lister
TCP	0.0.0.0:25	0.0.0.0:0	lister
TCP	0.0.0.0:80	0.0.0.0:0	lister
TCP	0.0.0.0:135	0.0.0.0:0	lister
TCP	0.0.0.0:443	0.0.0.0:0	lister
TCP	0.0.0.0:445	0.0.0.0:0	lister
TCP	0.0.0.0:1025	0.0.0.0:0	lister
TCP	0.0.0.0:1032	0.0.0.0:0	lister
TCP	0.0.0.0:1033	0.0.0.0:0	lister
TCP	0.0.0.0:1035	0.0.0.0:0	lister
TCP	0.0.0.0:1144	0.0.0.0:0	lister
TCP	0.0.0.0:1776	0.0.0.0:0	lister

**TCP Statistics:**

Retransmission time-out algorithm	vanj
Min. retransmission time-out (msec)	300
Max. retransmission time-out (msec)	120000
Max. number of connections	dynam
Active Opens	532
Passive Opens	67
Failed connection attempts	82

**UDP Statistics:**

Datagrams received	481
No ports	675
Receive errors	0
Datagrams sent	1155

**ICMP Statistics:**

	Received	Sent
Messages	674	4
Errors	0	0



# AWSPS: IP Statistics/ Settings

**AW Security Port Scanner 4.61 Professional**

File Run Utilities Help

**High-Power Network Tools** for all 32-bit Windows platforms

Ports Routing **IP/Transport Protocols** Interfaces Registry LAN Refresh  Auto 2 sec

**IP Statistics/Settings:**

Acting as IP router  
 Default TTL  
 Packets received  
 Received header errors  
 Received address errors  
 Datagrams forwarded  
 Unknown protocols received

**Installed Protocols:**

MSAFD Tcpip [TCP/IP]  
 MSAFD Tcpip [UDP/IP]

**Protocol Details:**

Address Family: AF\_INET  
 Protocol: IPPROTO\_TCP  
 Socket Type: SOCK\_STREAM  
 Connectionless: No  
 Guaranteed Delivery: Yes

**Addressing Information Table:**

IP	Interface index	Sub-net mask	LSB in IP non-unicast address	Largest IP datagram can reassemble
127.0.0.1	0x00000001	255.0.0.0	1	65535
192.168.1.100	0x00000002	255.255.255.0	1	65535

**Net to Media Table:**

Interface index	Media dependent physical address	IP address	Type of mapping
0x00000002	00-04-5A-EA-70-5F	192.168.1.1	dynamic

# AWSPS: UDP Scan

**AW Security Port Scanner 4.61 Professional**

File Run Utilities Help

Site: 192.168.1.101 Port: 138 Counter: 0

**Udp Scan**

**Opened Ports**

Remote Port	Service Port
19	chargen
135	epmap/loc-srv
137	netbios-ns
138	netbios-dgm

**Closed Ports**

Remote Port	Service Port
129	pwdgen
130	cisco-fna
131	cisco-tna
132	cisco-sys
133	statsrv
134	ingres-net
136	profile

**Events Report**

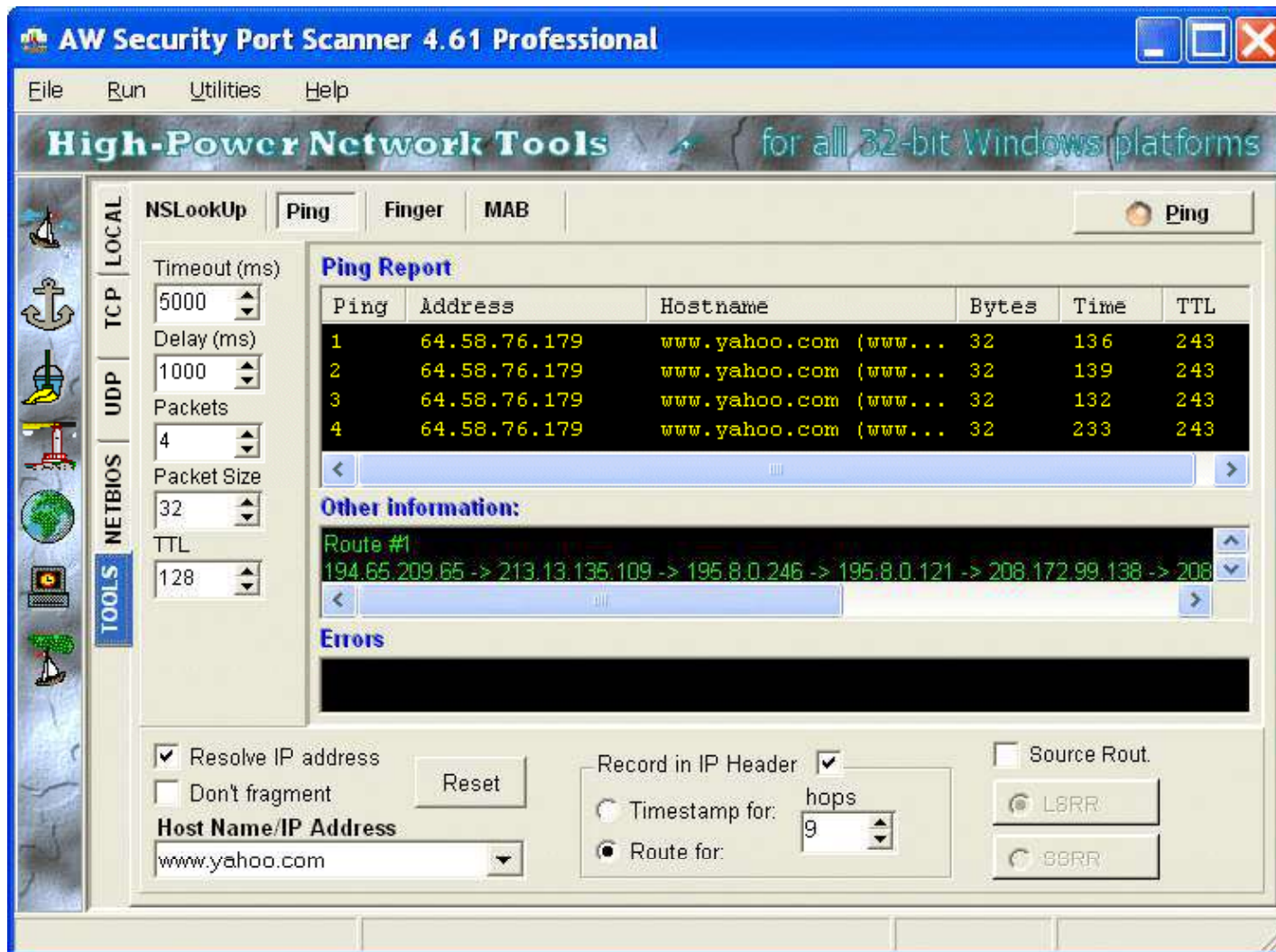
```
#10:18:31 AM New scanning.
#10:18:31 AM Testing probes, please wait some.
#10:18:31 AM Host UDP is responsive.
#10:18:31 AM Starting scan.
#10:18:35 AM Opened port 7, local port 2084.
Standard Service: Echo
#10:18:39 AM Opened port 9, local port 2087.
Standard Service: Discard (sink null)
#10:18:43 AM Opened port 13, local port 2092.
Standard Service: Daytime
```

Average RTT (sec): 0.004

Initial test probe  
 Smart probing  
 User selected

Probe Port: [ ]

Remote Host  
 Name: LOCALLINK  
 Aliases: [ ]  
 IPs: 192.168.1.101  
 HTTP Server (P80): None





IPEye is a command-line driven port scanner for Windows

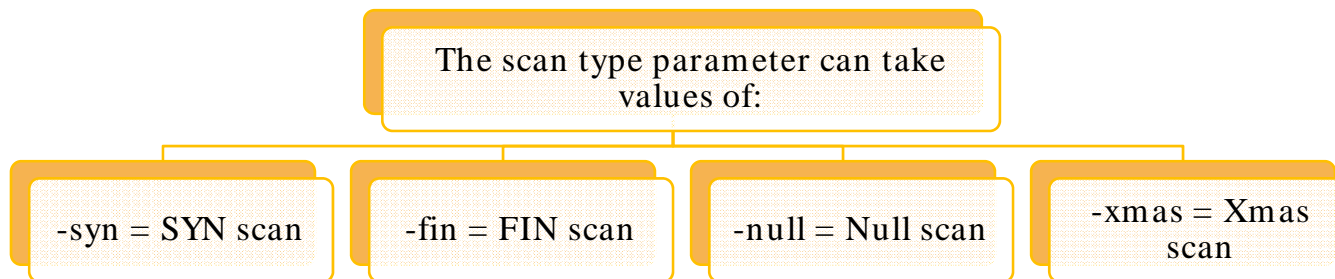
The basic usage for IPEye is:

```
ipEye <target IP> <scantype> -p <from port> <to port> [optional parameters]
```

Only SYN SCAN is valid when scanning a Windows system

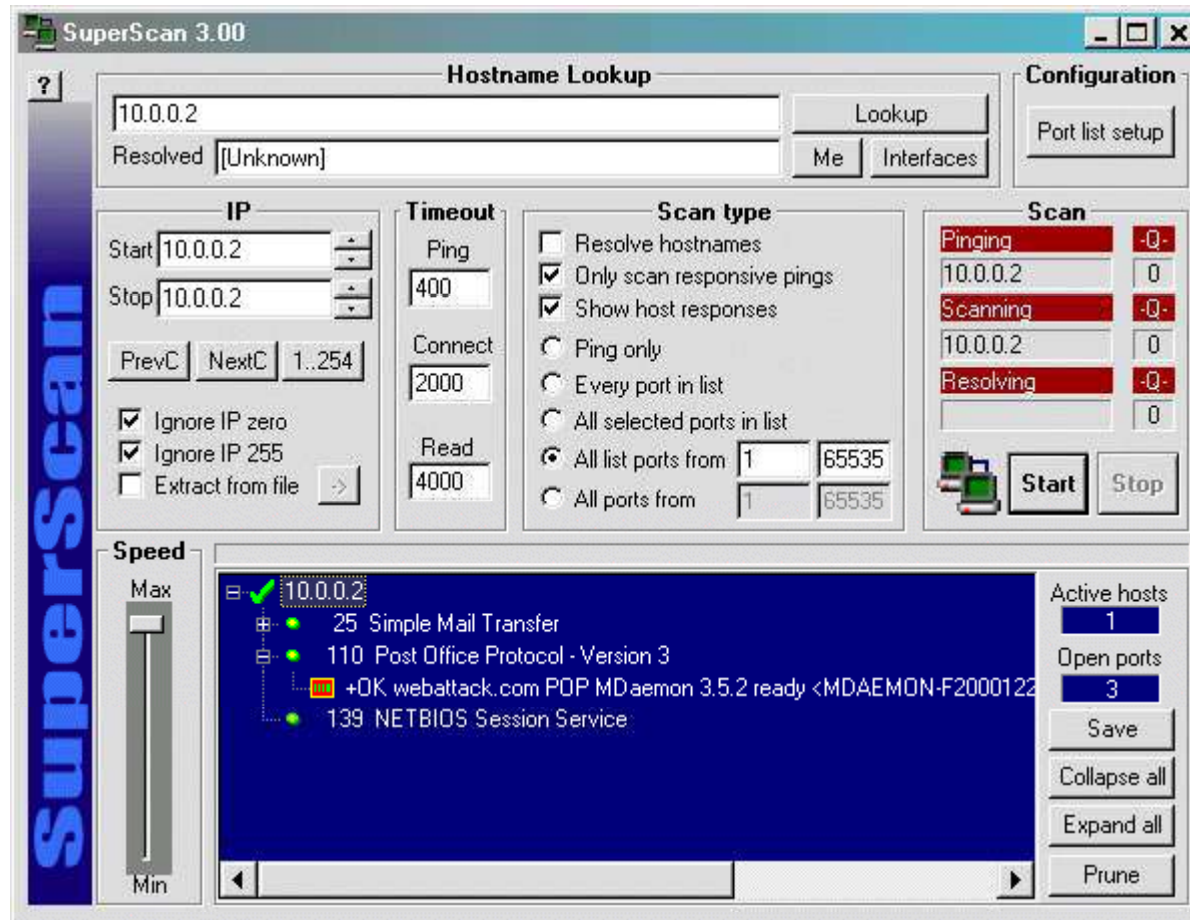
IPEye scans requested ports, given a valid IP address, and returns a list of ports which are open, closed, or rejected

IP address of the machine is required while scanning; host names are not accepted





# IPEye: Screenshot

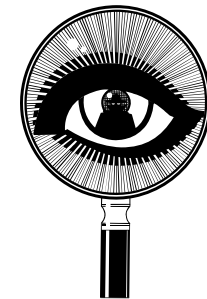


ike-scan is a command-line tool for discovering, fingerprinting, and testing IPsec VPN systems

It constructs and sends IKE Phase-1 packets to the specified hosts and displays any responses that are received

ike-scan allows to:

- Send IKE packets to any number of destination hosts
- Construct the outgoing IKE packet in a flexible way
- Decode and display any returned packets
- Crack aggressive mode pre-shared keys



# ike-scan: Screenshot 1

```
Shell - Konsole
BT ike-scan-1.8 # ls
AUTHORS                check-run3*           isakmp.h
COPYING                check-sizes.c         make-win32-zipfile.sh*
ChangeLog              config.h.in           md5.c
INSTALL                configure*            md5.h
Makefile.am            configure.ac           missing*
Makefile.in            depcomp*              mkinstalldirs*
NEWS                   error.c               pkt-custom-proposal.dat
README                 getopt.c              pkt-default-proposal.dat
README-WIN32           getopt.h              psk-crack-dictionary
TODO                   getopt1.c             psk-crack.l
acinclude.m4           ike-backoff-patterns psk-crack.c
aclocal.m4             ike-scan.l            sha1.c
check-hash.c           ike-scan.c            sha1.h
check-packet*          ike-scan.h            udp-backoff-fingerprinting-paper.tx
check-psk-crack-1*     ike-vendor-ids        utils.c
check-psk-crack-2*     inet_aton.c           wrappers.c
check-run1*            install-sh*
check-run2*            isakmp.c
BT ike-scan-1.8 # grep -R ike-scan-target.test.nta-monitor.com *
ike-scan.c:            hp = gethostbyname("ike-scan-target.test.nta-monitor.com");
BT ike-scan-1.8 #
```

# ike-scan: Screenshot 2

```
Shell - Konsole <2>
BT ike-scan-1.9 # ls
AUTHORS                config.status*       pkt-aggr-mode-response.dat
COPYING                configure*            pkt-aggressive.dat
ChangeLog              configure.ac          pkt-checkpoint-notify.dat
INSTALL                depcomp*             pkt-custom-proposal.dat
Makefile               error.c              pkt-default-proposal.dat
Makefile.am            error.o              pkt-ikev2.dat
Makefile.in            getopt.c             pkt-main-mode-response.dat
NEWS                   getopt.h             pkt-main-natt-response.dat
README                 getopt1.c            pkt-malformed.dat
README-WIN32           hash_functions.h     pkt-notify-response.dat
TODO                   ike-backoff-patterns pkt-single-trans.dat
acinclude.m4           ike-scan*            pkt-v2-notify-response.dat
aclocal.m4             ike-scan.l           pkt-v2-sainit-response.dat
check-decode*          ike-scan.c           psk-crack*
check-hash*            ike-scan.h           psk-crack-dictionary
check-hash.c           ike-scan.o           psk-crack.l
check-hash.o           ike-vendor-ids      psk-crack.c
check-packet*          inet_aton.c          psk-crack.h
check-psk-crack-1*     install-sh*          psk-crack.o
check-psk-crack-2*     ip.h                 shal.c
check-psk-crack-3*     isakmp.c             shal.h
check-psk-crack-4*     isakmp.h             shal.o
check-run1*            isakmp.o             stamp-h1
check-run2*            make-win32-zipfile.sh* udp-backoff-fingerprinting-paper.txt
check-run3*            md5.c                udp.h
check-sizes*           md5.h                utils.c
check-sizes.c          md5.o                utils.o
check-sizes.o           missing*             wrappers.c
config.h               mt19937ar.c*         wrappers.o
config.h.in            mt19937ar.o
config.log             pkt-aggr-cert-response.dat
BT ike-scan-1.9 # grep -R ike-scan-target.test.nta-monitor.com *
BT ike-scan-1.9 #
```

Infiltrator is an intuitive network security scanner that can quickly scan and audit your network computers for vulnerabilities, exploits, and information enumerations

## Features:

Information Gathering

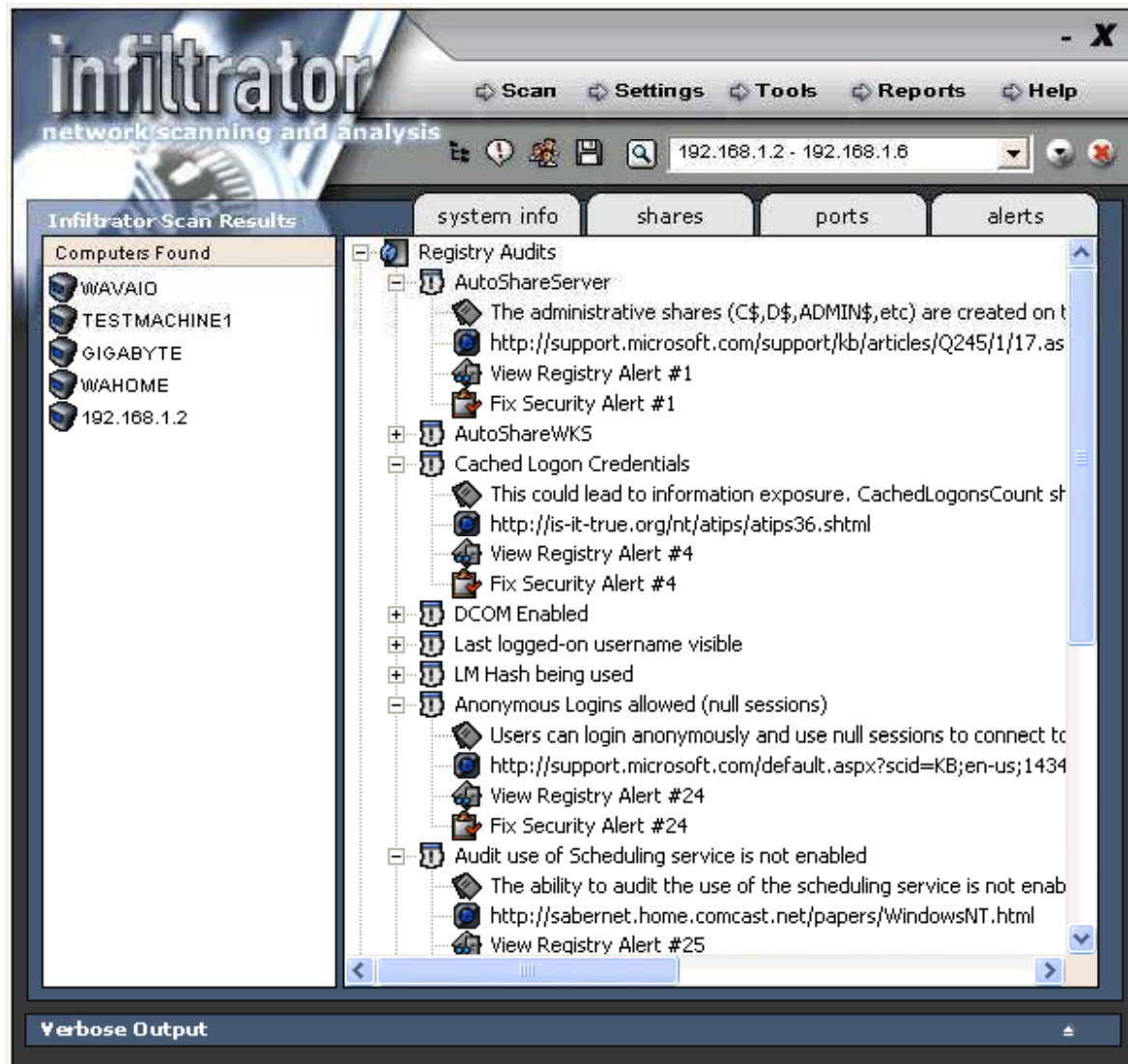
Security Auditing and Analysis

Generates Sleek Scan Reports

Comes with many built in network utilities such as Whois client



# Infiltrator Network Security Scanner: Screenshot 1



# Infiltrator Network Security Scanner: Screenshot 2



Yaps is a small and fast TCP/IP port scanner with little configuration options and a fairly plain interface

## Features:

Supports simultaneous connections to many targets

Supports command line and GUI mode

Customizable timeout

Can scan a range of addresses or single address

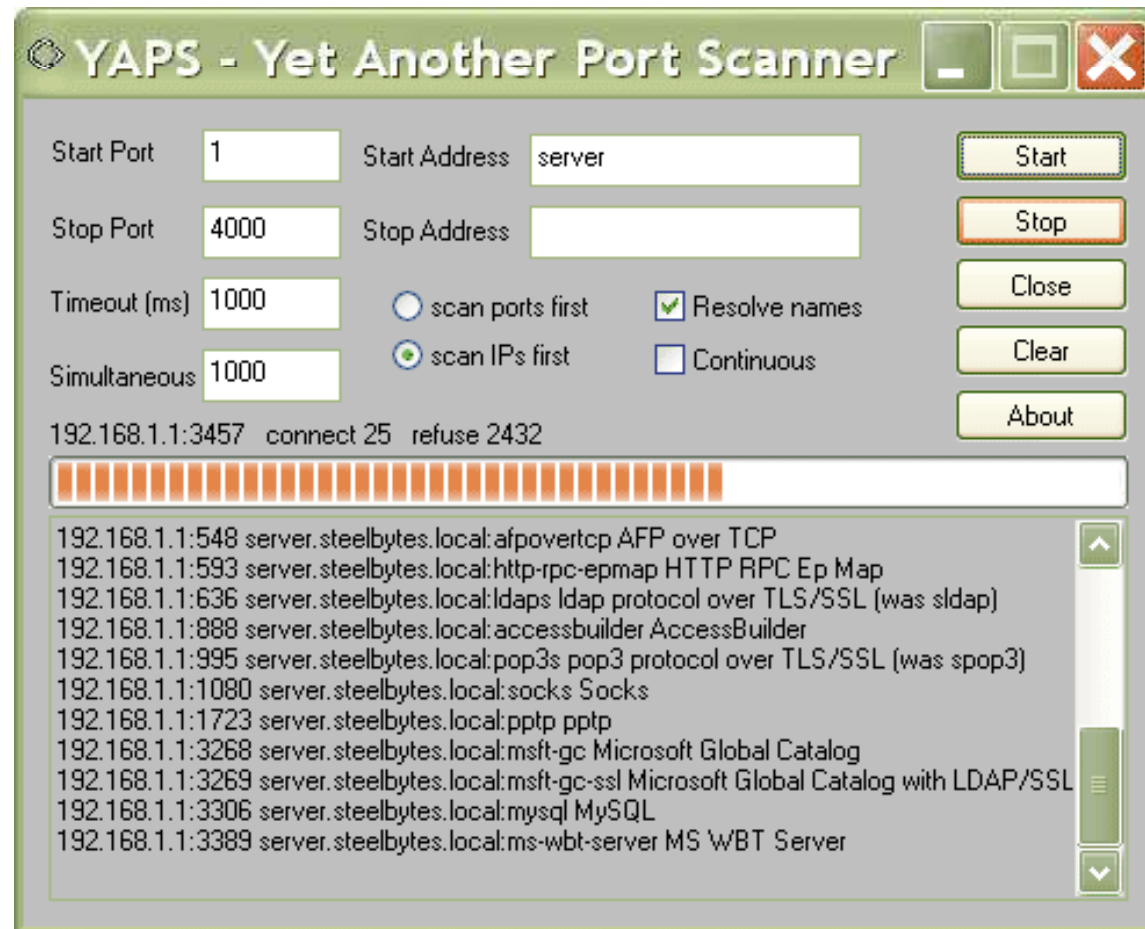
Can resolve addresses

Includes names for well known ports





# YAPS: Yet Another Port Scanner: Screenshot



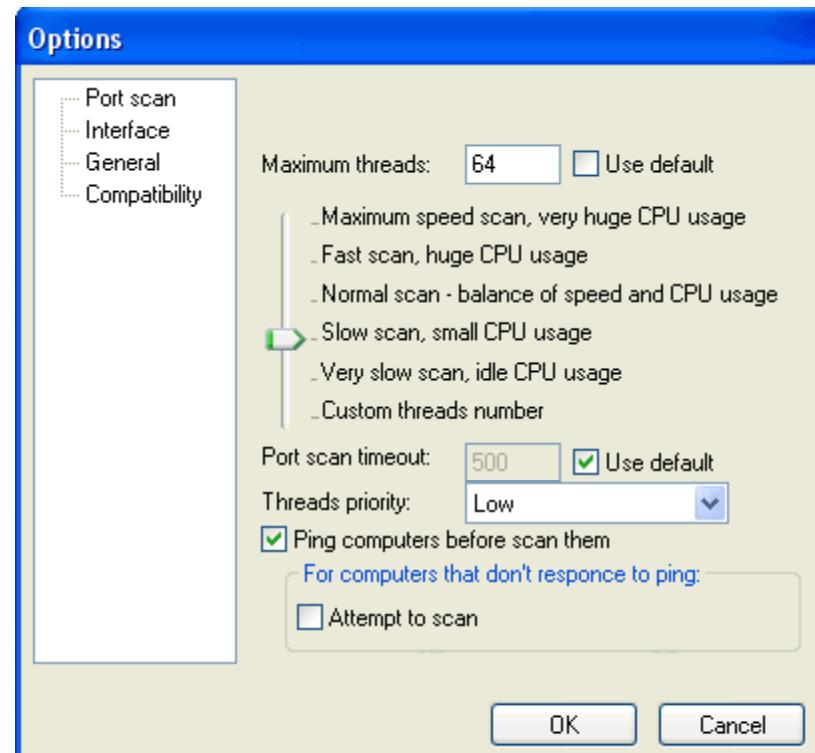
Advanced Port Scanner is a small, fast, and easy-to-use port scanner that runs multi-threaded for optimum performance

## Features:

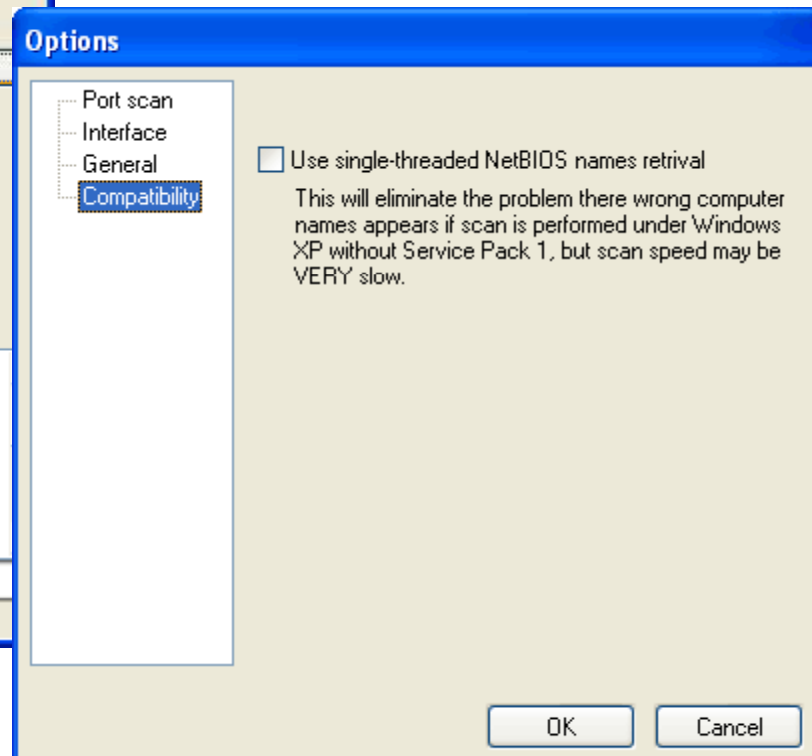
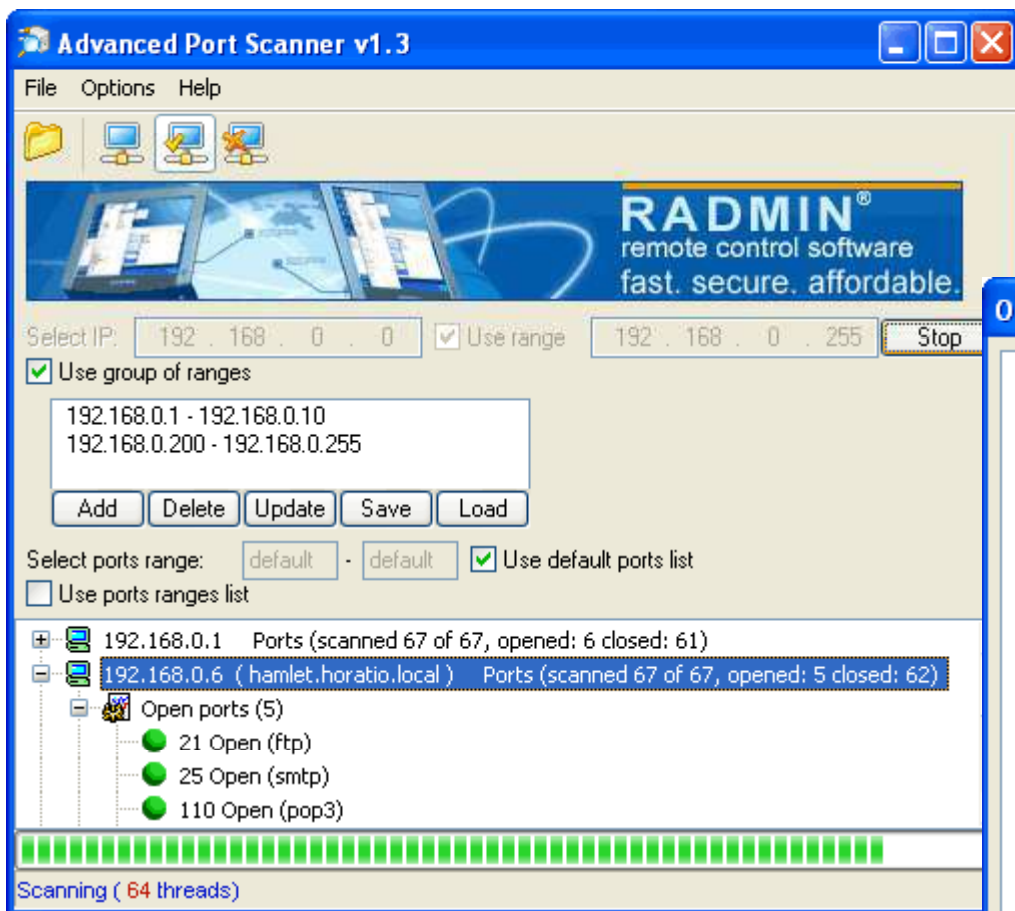
Fast and Stable multi-threaded Port Scanning

Fully configurable Port Scan

Export scan results



# Advanced Port Scanner: Screenshots



NetworkActiv Port Scanner is a network exploration and administration tool that allows you to scan and explore internal LANs and external WANs

## Features:

- TCP connect() port scanner and TCP SYN port scanner
- UDP port scanner with automatic speed control
- Ping scanning of subnets (UDP or ICMP)
- TCP subnet port scanner for finding Web servers and other servers
- High performance trace-route
- Remote OS detection by TCP/IP stack fingerprinting
- Whois Client
- DNS Dig system

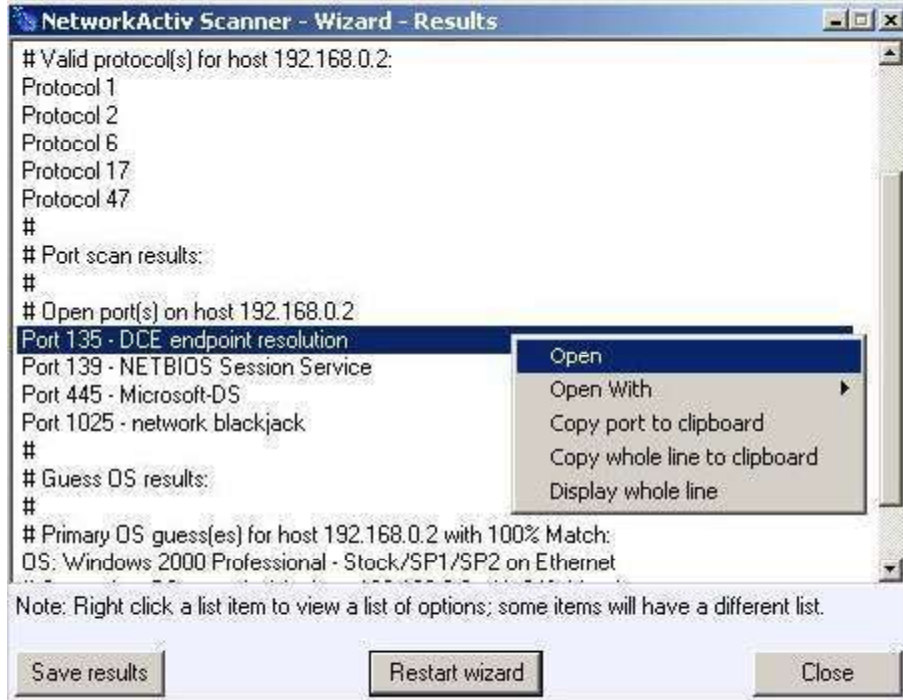
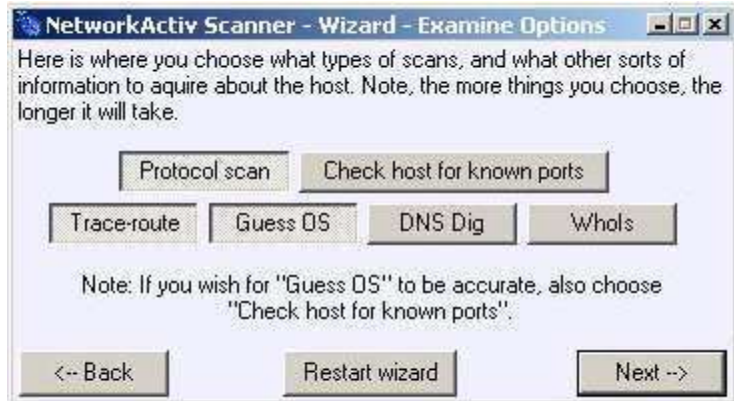
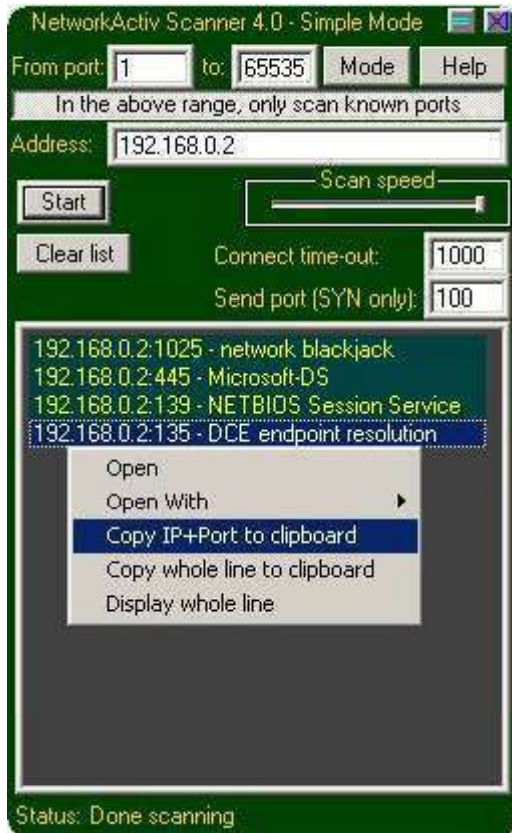


# NetworkActiv Scanner: Screenshot 1





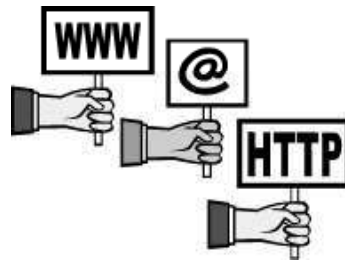
# NetworkActiv Scanner: Screenshot 2



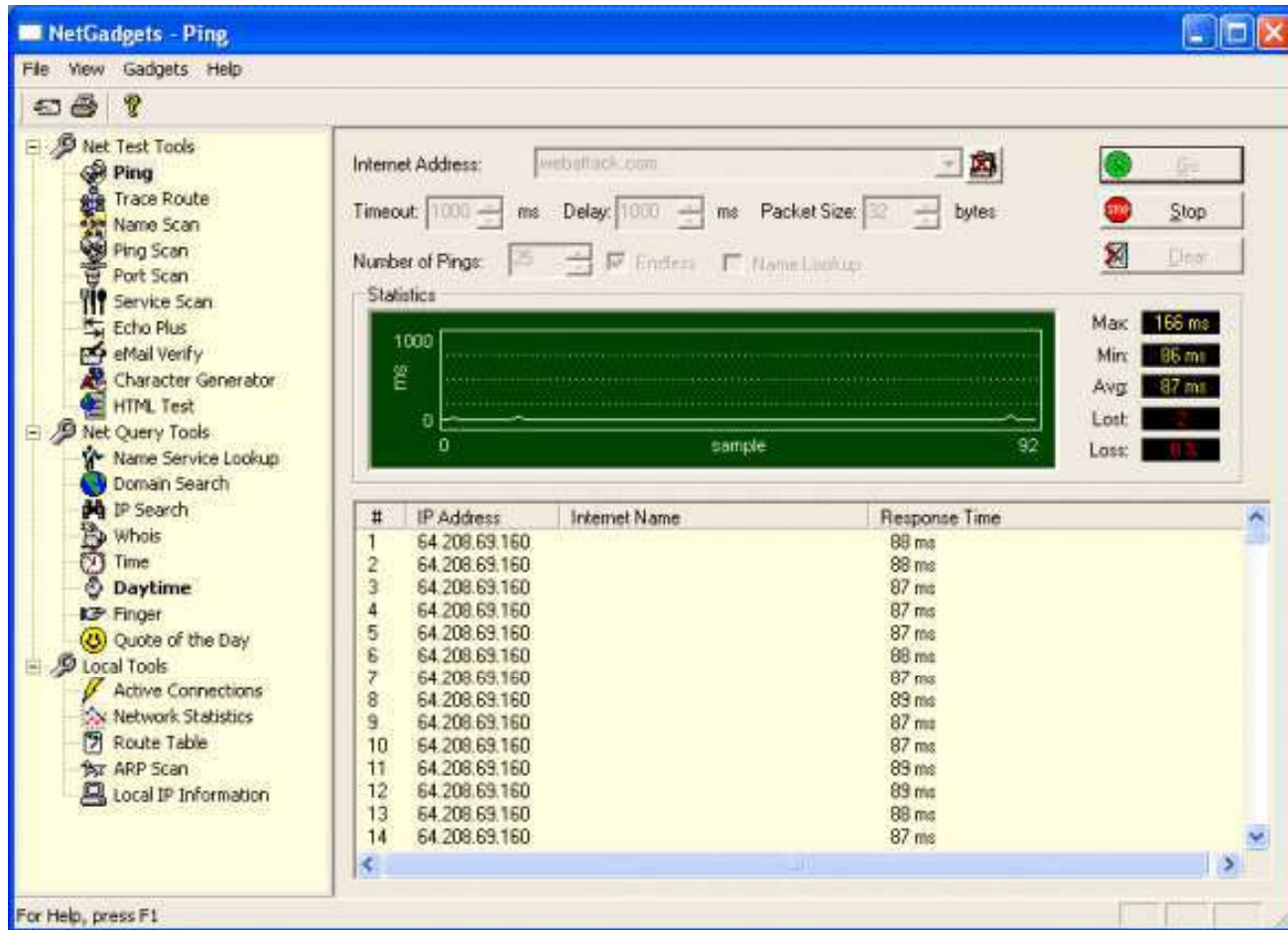
NetGadgets is a complete set of diagnostic tool for every level of Internet user

The tools within NetGadgets provide invaluable data about your Internet and network connections, other users, and web site information

It combines all the standard Internet tools like Ping, Trace Route, NS Lookup and Whois, with other less common tools like Time, Daytime, Echo Plus, Email Verify, Finger, Name Scan, Ping Scan, Port Scan, Service Scan, and others



# NetGadgets: Screenshot





# P-Ping Tools

P-Ping Tools is an administrative network scanner that allows you to scan TCP/UDP ports to see if they are in use

You can scan a single or multiple IP address and also log the results to a text file that are in use

The program allows you to scan a single port or all of them, as well as scanning for popular services on an IP range

# P-Ping Tools: Screenshot



MegaPing is the ultimate must-have toolkit that provides all essential utilities for Information System specialists, system administrators, IT solution providers, or individuals

## Features:

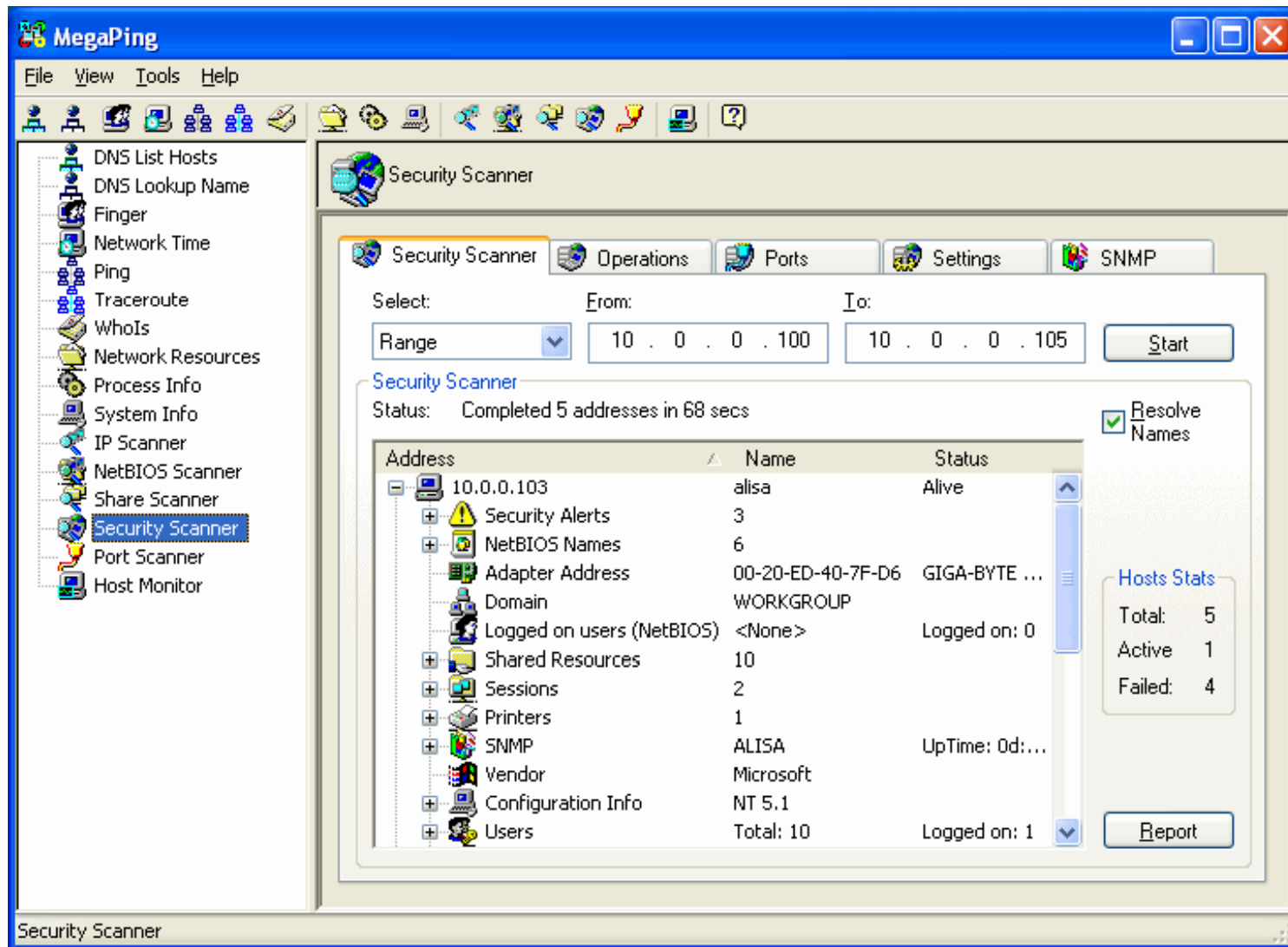
Includes scanners, host and port monitors, system information viewers, and various network utilities

Automatically detects security vulnerabilities on your network

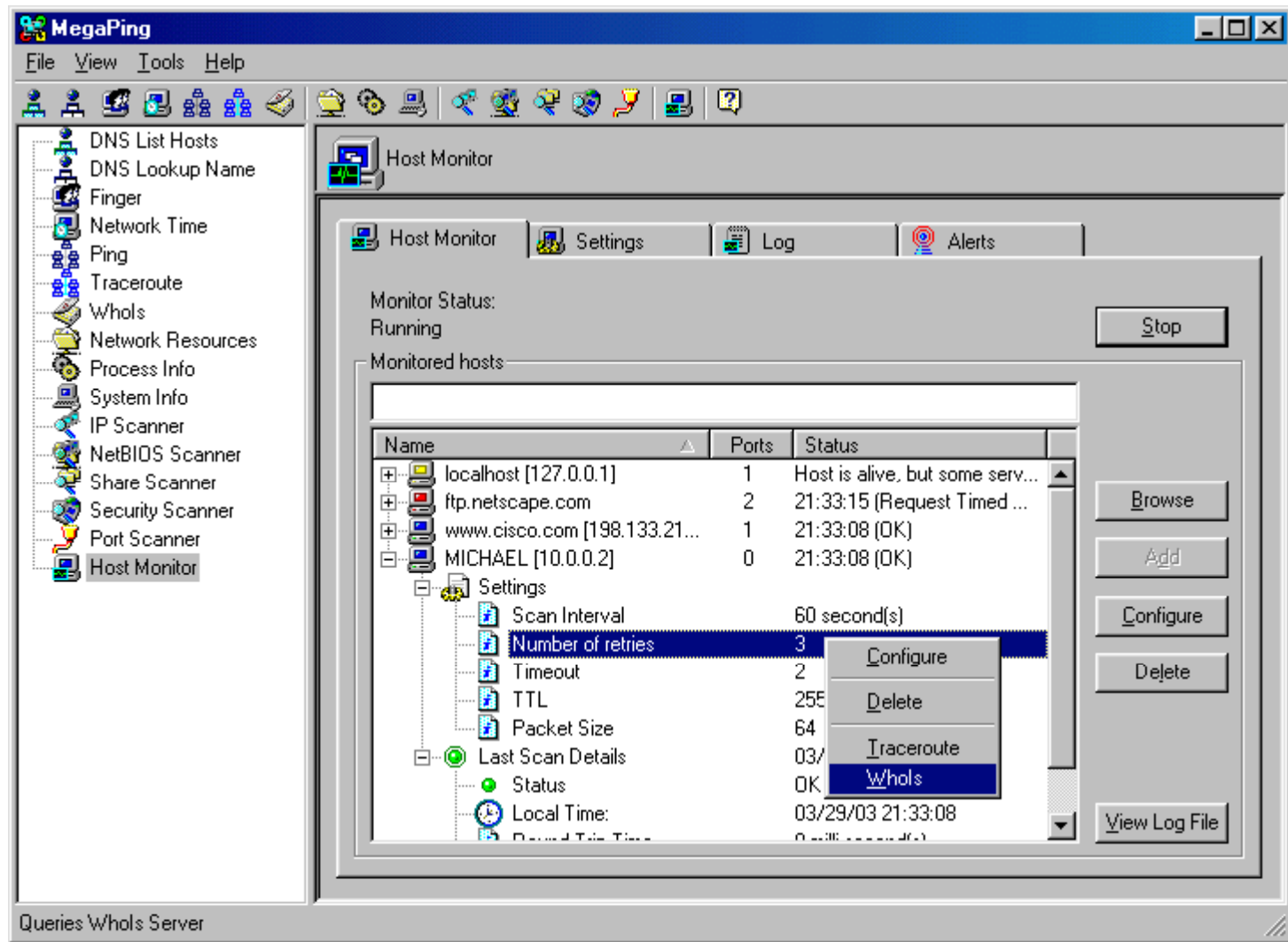
Provides detailed information about all computers and network appliances



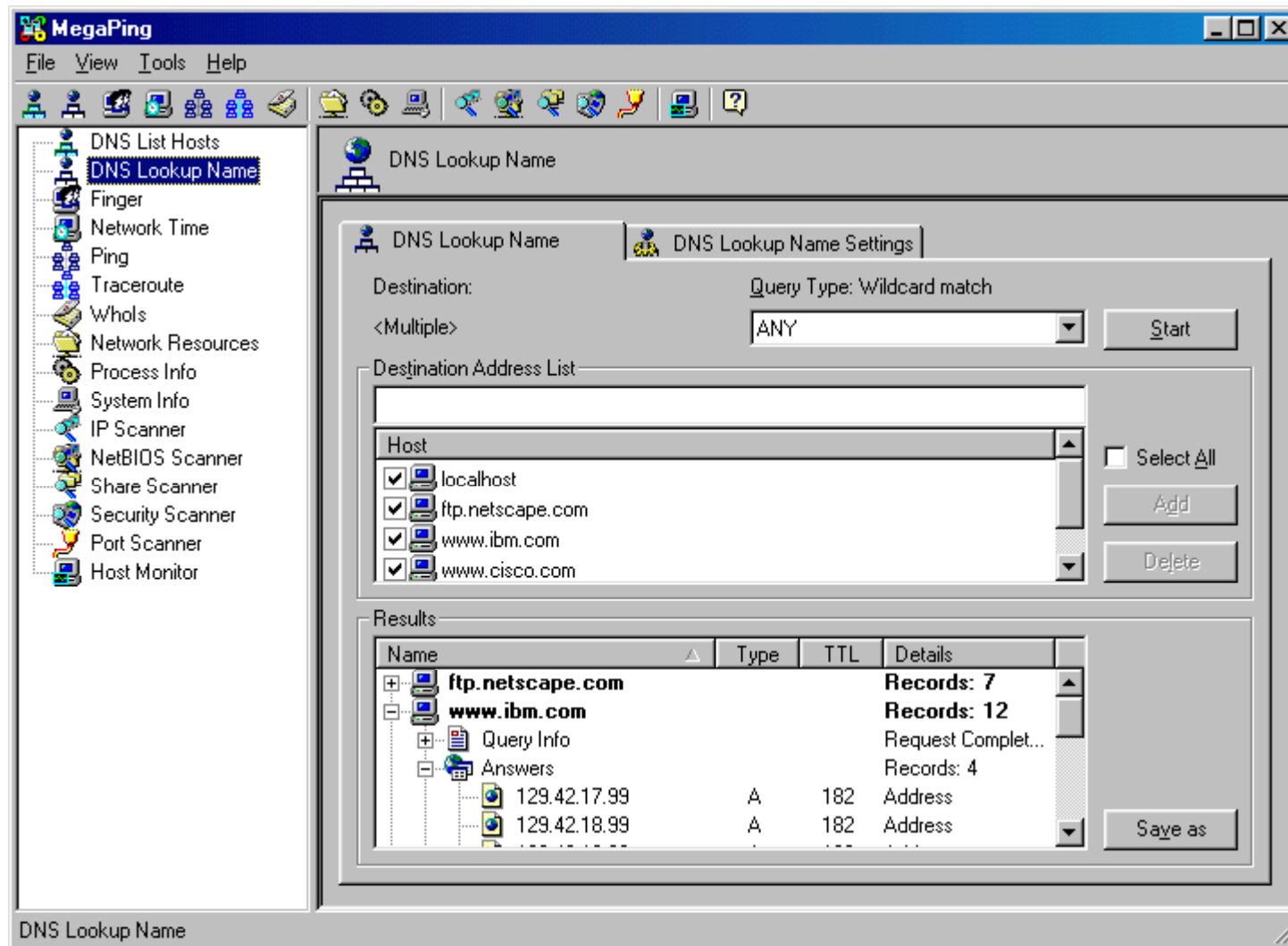
# MegaPing: Screenshot 1



# MegaPing: Screenshot 2



# MegaPing: Screenshot 3



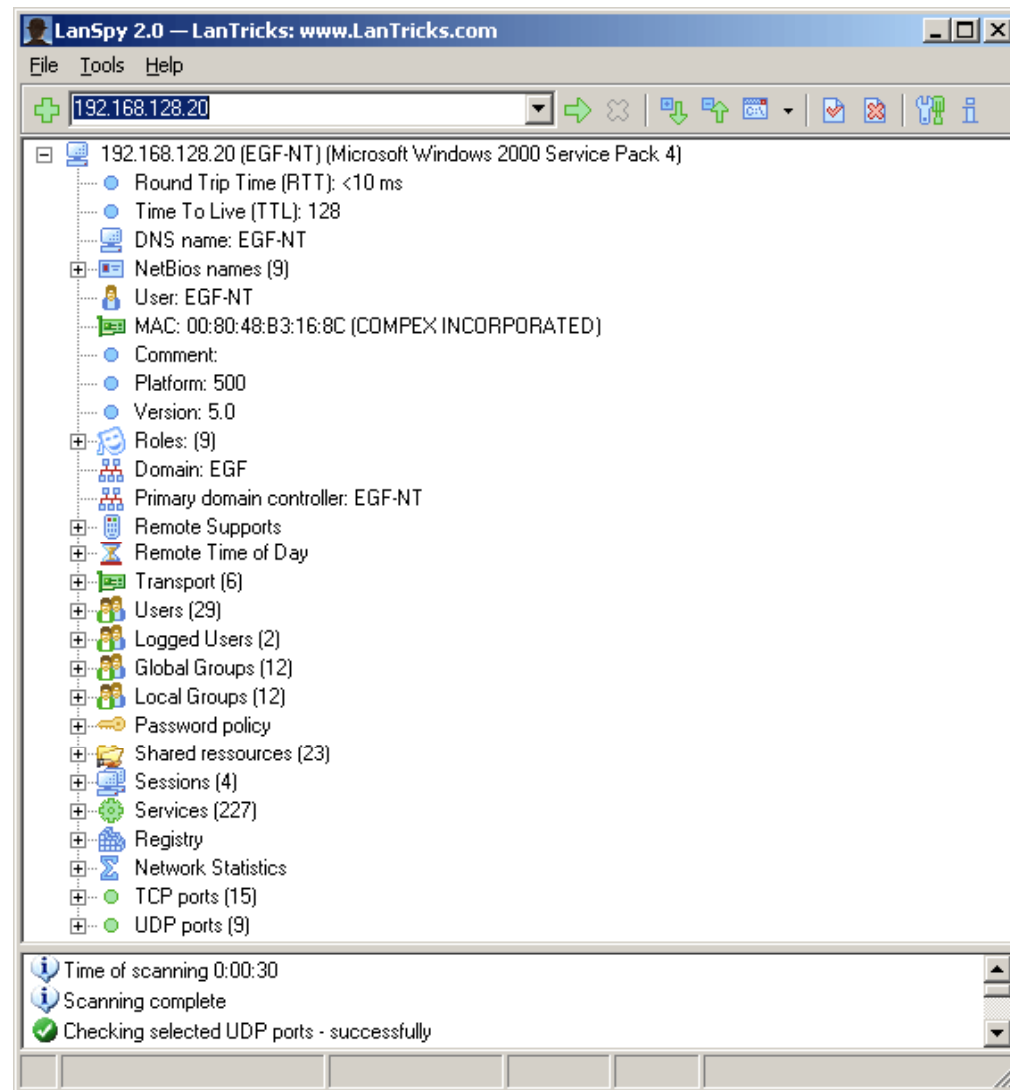
LanSpy is a set of network utilities pooled together in a single program with simple and easy-to-use interface

It includes fast port scanner for gathering information about open ports on remote computer and displays services using these ports

## Features:

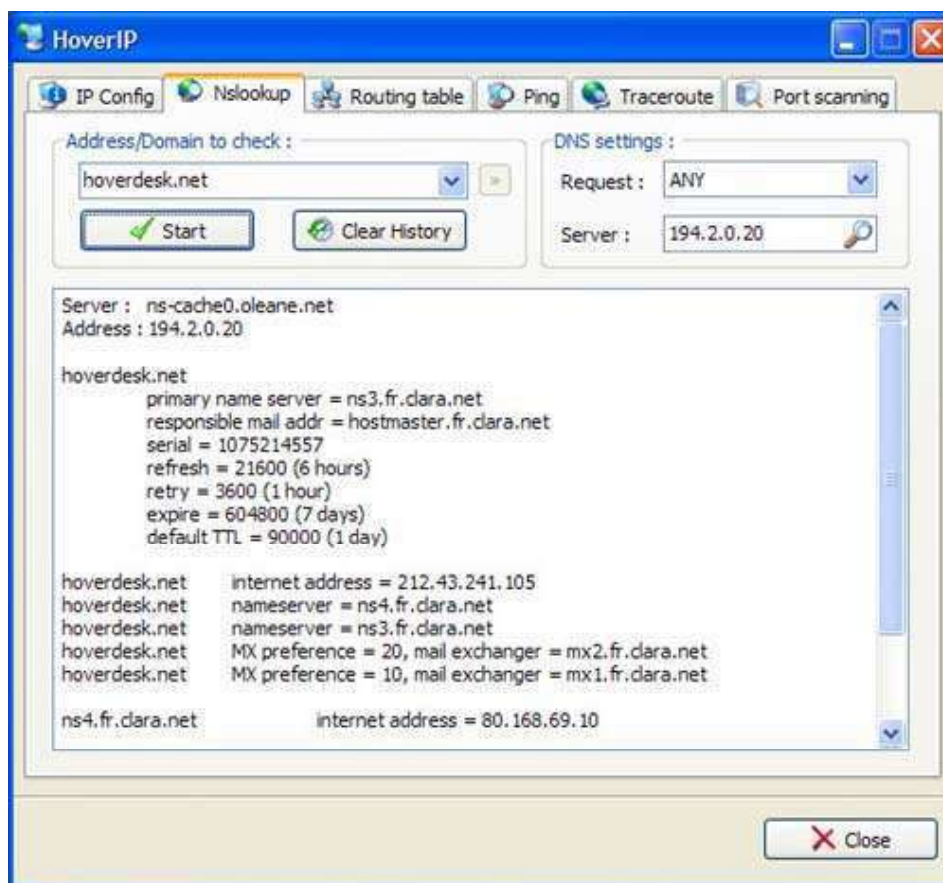
- Audits your network for security reason issues
- Views processes on remote computers
- Shows a list of installed application on workstations
- Detects shares, open ports, and user accounts

# LanSpy: Screenshot





HoverIP is a useful set of network utilities, that can display your IP configuration (on all network cards), perform NsLookup queries, Traceroute, Ping, and port scanning



# HoverIP: Screenshot

The screenshot shows the HoverIP application window with the 'Traceroute' tab selected. The host being traced is 'www.hoverdesk.net'. The 'Perform Reverse Lookup' option is checked. The traceroute results are displayed in a table with columns for Hop, IP, Time, TTL, Info, and Hostname.

Hop	IP	Time	TTL	Info	Hostname
1	192.168.0.1	0ms	255	OK	
2	193.253.160.3	60ms	126	OK	
3	80.10.168.196	60ms	252	OK	GE4-479.ncidf104.Paris.francet...
4	193.252.159.34	50ms	252	OK	pos12-0.nrsta104.Paris.francet...
5	193.251.126.102	50ms	251	OK	pos12-1.ntsta202.Paris.francet...
6	193.251.126.70	60ms	250	OK	pos14-0.ntsta302.Paris.francet...
7	193.252.103.117	60ms	248	OK	pos0-0-0-0.nosta102.Paris.fran...
8	198.32.247.83	60ms	248	OK	Claranet-8975.tlh.giga.parix.net
9	212.43.193.22	60ms	241	OK	fe-2-0-th2-fett.rtr.fr.clara.net
10	212.43.193.246	60ms	242	OK	fe-0-0-0-th2-zuckuss.rtr.fr.clar...
11	212.43.193.181	60ms	245	OK	ge-2-0-fbg-ig88.rtr.fr.clara.net
12	212.43.247.145	60ms	53	OK	fe-0-kala.rtr.fr.clara.net
13	212.43.241.105	60ms	243	DONE!	myhome0.fr.clara.net

Status: idle

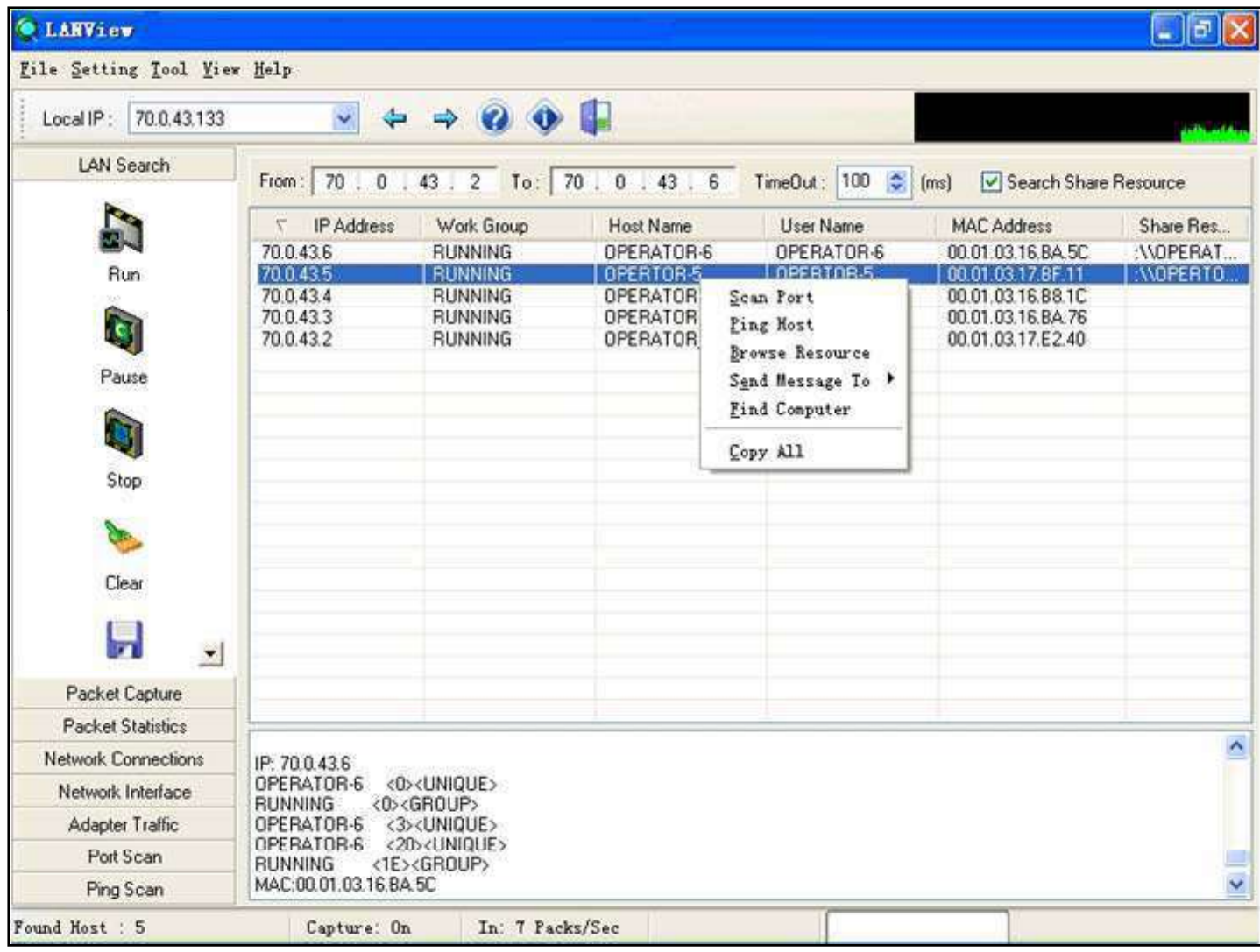
LANView can quickly obtain information about all hosts on a network, including IP addresses, MAC addresses, hostnames, users, and groups

## Features:

- Multiple applications in one: LAN Search, capturing and analyzing IP packets
- IP Statistics, IP Traffic, Network Connections, Port Scan, Ping Scan, Local interface, and Windows Socket information, organized as independent windows allow multitask operation
- Multiple thread design ensures the efficiency
- LAN Searcher, IP Capture, Port Scan, Ping Scan, and some other functions are designed as independent threads



# LANView: Screenshot 1



# LANView: Screenshot 2

LANView

File Setting Tool View Help

Local IP: 71.0.33.36

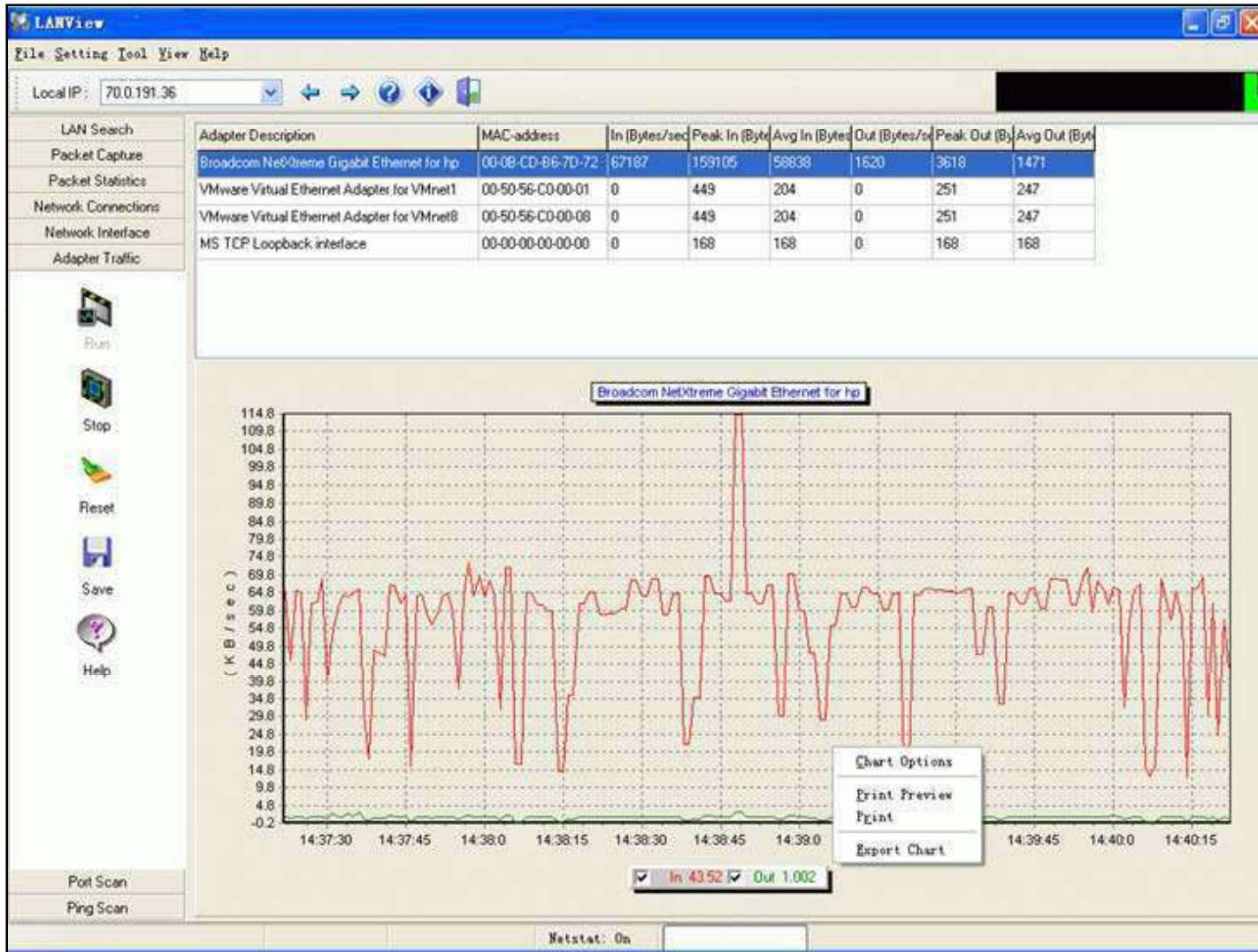
IP Address: 71 . 0 . 33 . 236

Open Port	Protocol	Description
1	TCP	TCP port multiplexer (RFC 1078);
457	TCP	
80	TCP	World Wide Web HTTP;
111	TCP	SUN Remote Procedure Call;
139	TCP	NetBIOS Session Service;
1018	TCP	
1032	TCP	
1033	TCP	
615	TCP	
620	TCP	
199	TCP	

Found Host : 22    Capture: On    In: 747 Packs/Sec    Netstat: On



# LANView: Screenshot 3



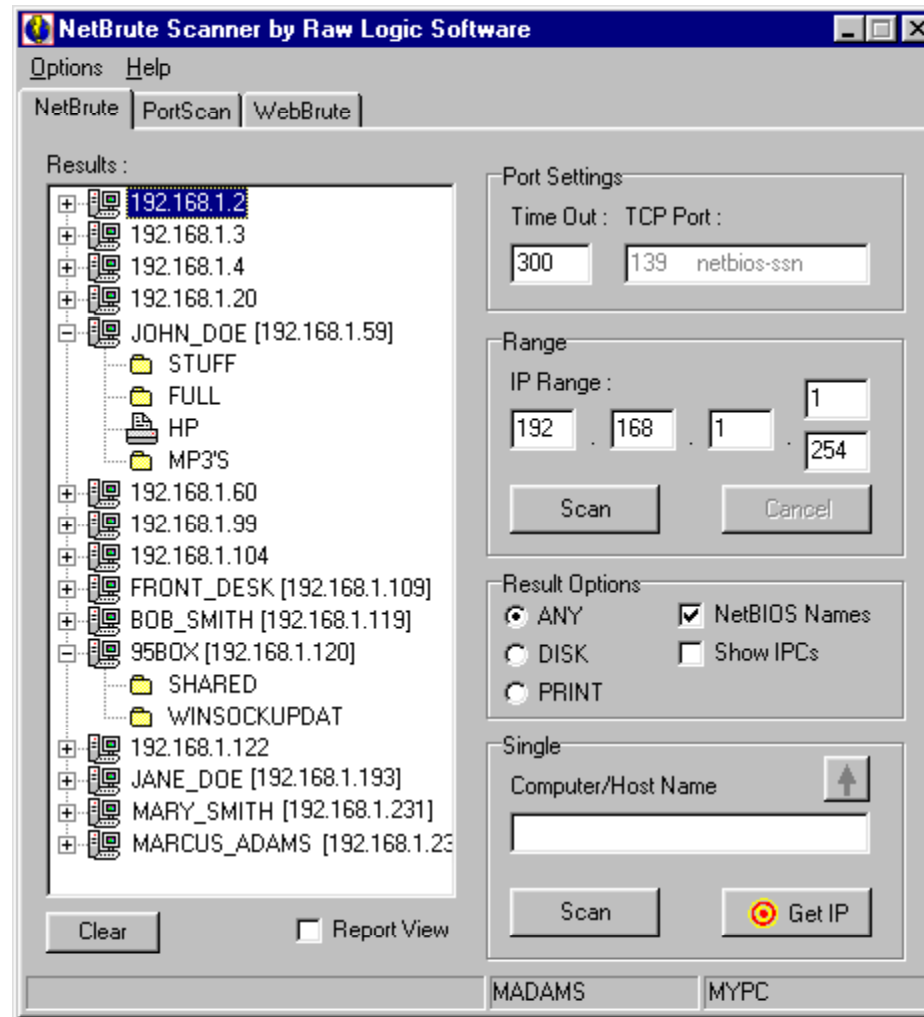
NetBrute allows you to scan a single computer or multiple IP addresses for available Windows File & Print Sharing resources

- This is probably one of the most dangerous and easily exploitable security holes

It is common for novice users to have their printers or their entire hard drive shared without being aware of it

This utility will help you to find these resources, so you can secure them with a firewall or by informing your users how to properly configure their shares with tighter security

# NetBruteScanner: Screenshot



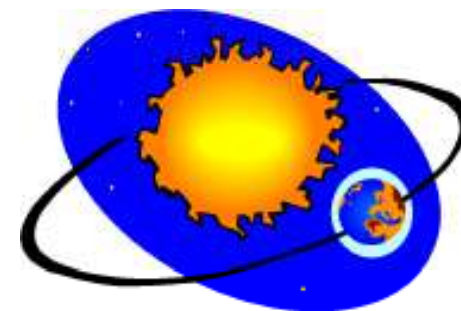


# SolarWinds Engineer's Toolset

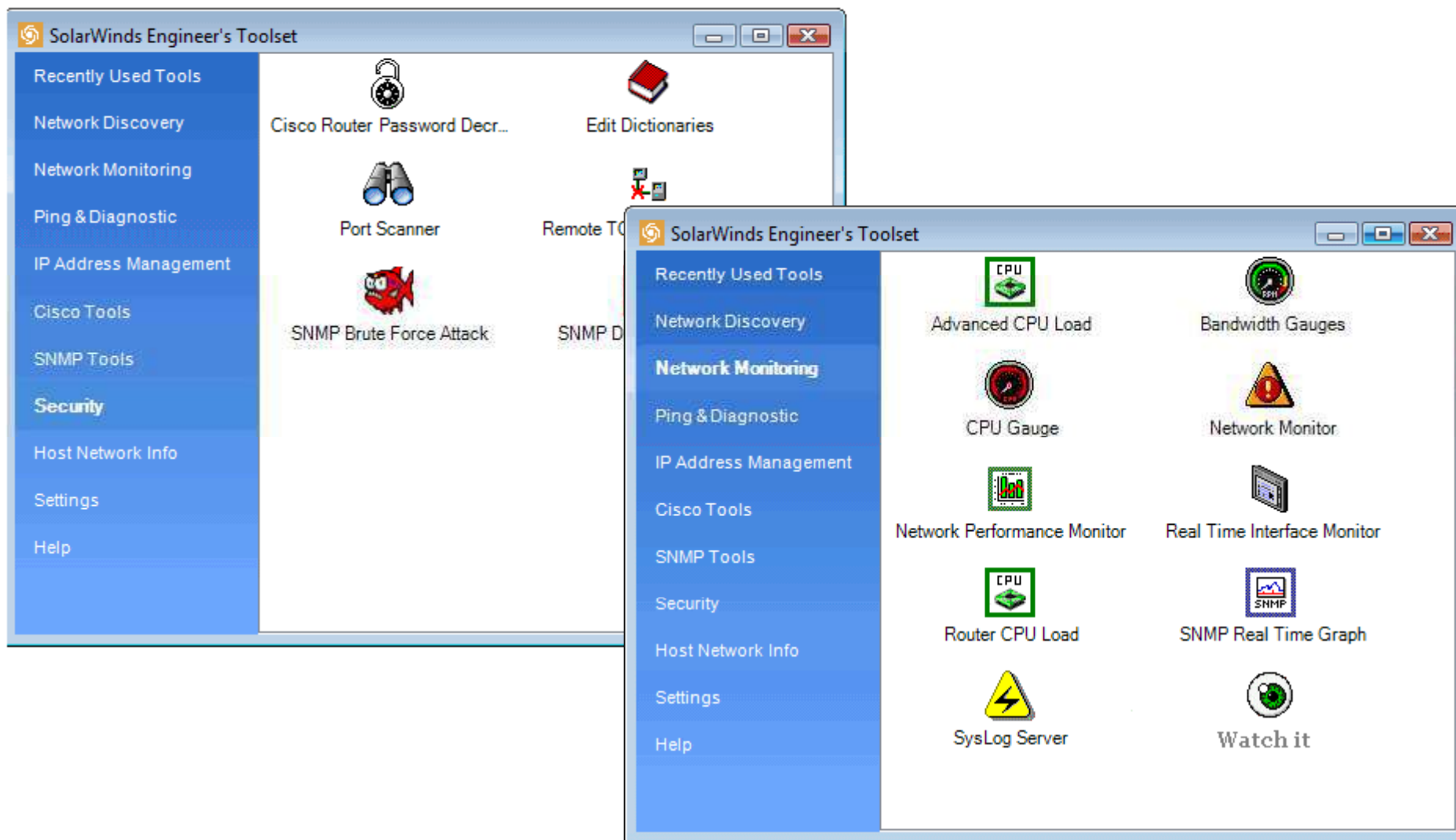
Engineer's Toolset includes 49 powerful network management, monitoring and troubleshooting tools to easily and effectively manage your network

## Features:

- Monitors and alerts on availability, bandwidth utilization, and health for hundreds of network devices
- Provides robust network diagnostics for troubleshooting and quickly resolving complex network issues
- Offers an array of network discovery tools that facilitate IP address management, port mapping and ping sweeps
- Eases management of Cisco® devices with tools for real-time NetFlow analysis, configuration management and router management



# SolarWinds Engineer's Toolset: Screenshots



NetworkActiv AUTAPF is easy to use, and quick to configure UDP and TCP Windows based port forwarder

## Features:

- Define IP address ranges to allow or block for each port being forwarded
- Optionally control IP address filtering via external program or script - in real-time
- **Have program forward multiple ports simultaneously**
- View the current data throughput speed of each port forwarding operation
- **Have program log connection events to a text file**
- **Have program hide in taskbar**



# AUTAPF: Screenshots

**NetworkActiv AUTAPF**

File Settings Help

Global status:

Current number of threads: 6  
 Current number of sessions: 1

New Edit Delete

Start Stop

Status of currently selected operation:

Current number of threads: 3  
 Current number of sessions: 1  
 Total number of sessions since start: 1  
 Total data from client side since start: 78 Bytes  
 Current data rate from client side: 0 bps  
 Total data from server side since start: 1.59 MB  
 Current data rate from server side: 186.21 Kbps

Port forwarding operations:

Status	Protocol	Local IP	Local port	Forw
Started	TCP	192.168.0.1	80	www

**Filter options for this port forwarding operation**

Host name resolver (use this to obtain the IP addresses needed):

www.networkactiv.com Resolve Reverse resolve Copy to filters

Only allow these IP address ranges:

From: 10 . 0 . 1 . 0 Add  
 To: 10 . 0 . 2 . 0 Remove

Load filter profile  
 Save filter profile

Block these IP address ranges:

From: 192 . 168 . 0 . 6 Add  
 To: 192 . 168 . 0 . 6 Remove

10.0.1.0 - 10.0.2.0  
 192.168.0.0 - 192.168.0.255  
 216.55.128.31 - 216.55.128.31

192.168.0.6 - 192.168.0.6

Clear all fields

Apply filters to incoming sessions.

OK Cancel

# OstroSoft Internet Tools

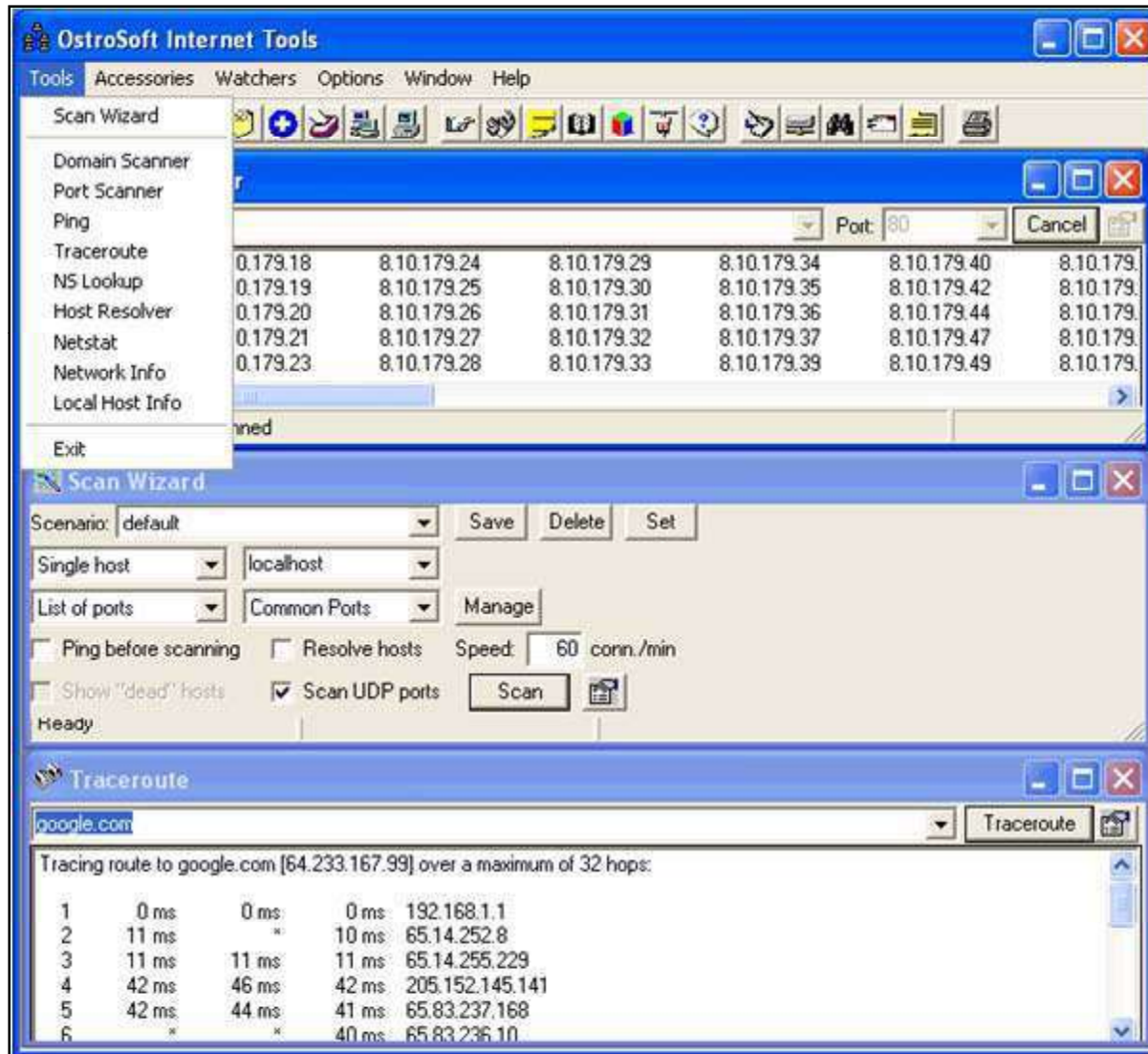
OstroSoft Internet Tools is an integrated set of network information utilities

It is intended for use by network, domain and systems administrators, network security professionals, Internet users, and everyone who wants to know more about network and Internet

It gives you vital information such as:

- Which computers on domain are running a specified service (domain scanner)
- What network services are running on aspecified computer (remote or local) - (Port scanner)
- Shows you the path TCP packet takes from your system to the remote host (Traceroute)
- Shows you the information about active connections on your computer (Netstat)
- Resolves host names to IP addressesand vice versa (Host Resolver - dns)
- Returns contact information (address,phone, fax, administrator name, DNS servers) for specified network (Network Info)
- Shows network-related information (IP address, host name, version of Winsock, etc.) about your computer (Local Host Info)

# OstroSoft Internet Tools: Screenshot



Advanced IP Scanner is a fast, robust, and easy to use LAN scanner, which gathers various types of information about the local network computers

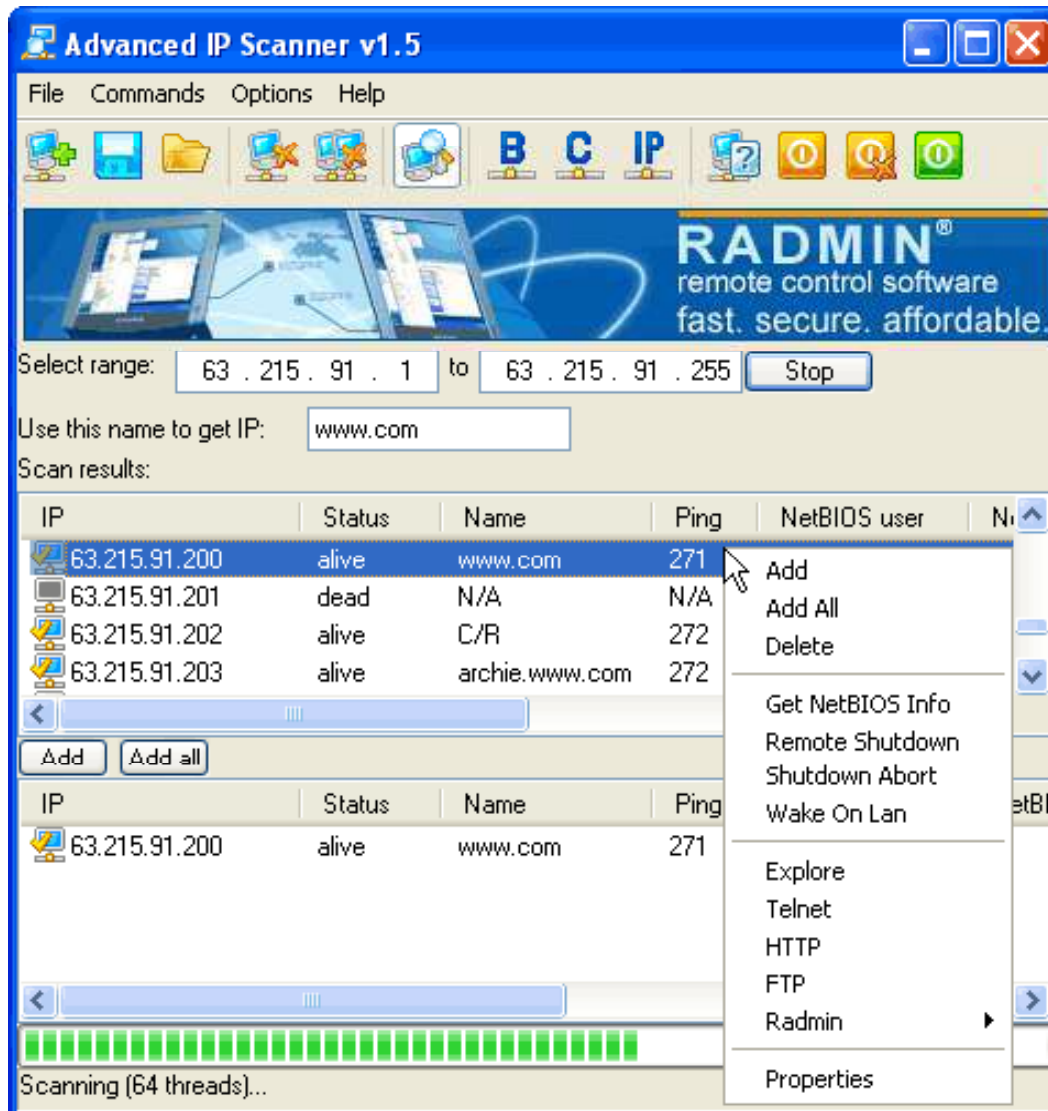
It provides access to many useful functions including remote shutdown and wake up

Results include NetBios username, computer name, group name, and Mac address

IP addresses can be saved in a list as well for later usage



# Advanced IP Scanner: Screenshot 1





# Advanced IP Scanner: Screenshot 2

**Computer properties**

IP: 63 . 215 . 91 . 200

Name: www.com

MAC: 00.00.00.00.00.00

Ping: 269

**NetBIOS info**

User name:

Computer name:

Group name:

Comments:

Current operation:

**Options**

- Remote Shutdown
- IP Scan
- General
- Lists**
- Radmin
- Compatibility

**Computers lists customization**

Choose list:

Show following rows for this list:

- IP
- Status
- Name
- Ping time
- NetBIOS user name
- NetBIOS computer name
- NetBIOS group name
- NetBIOS MAC address
- Comment

# Colasoft MAC Scanner

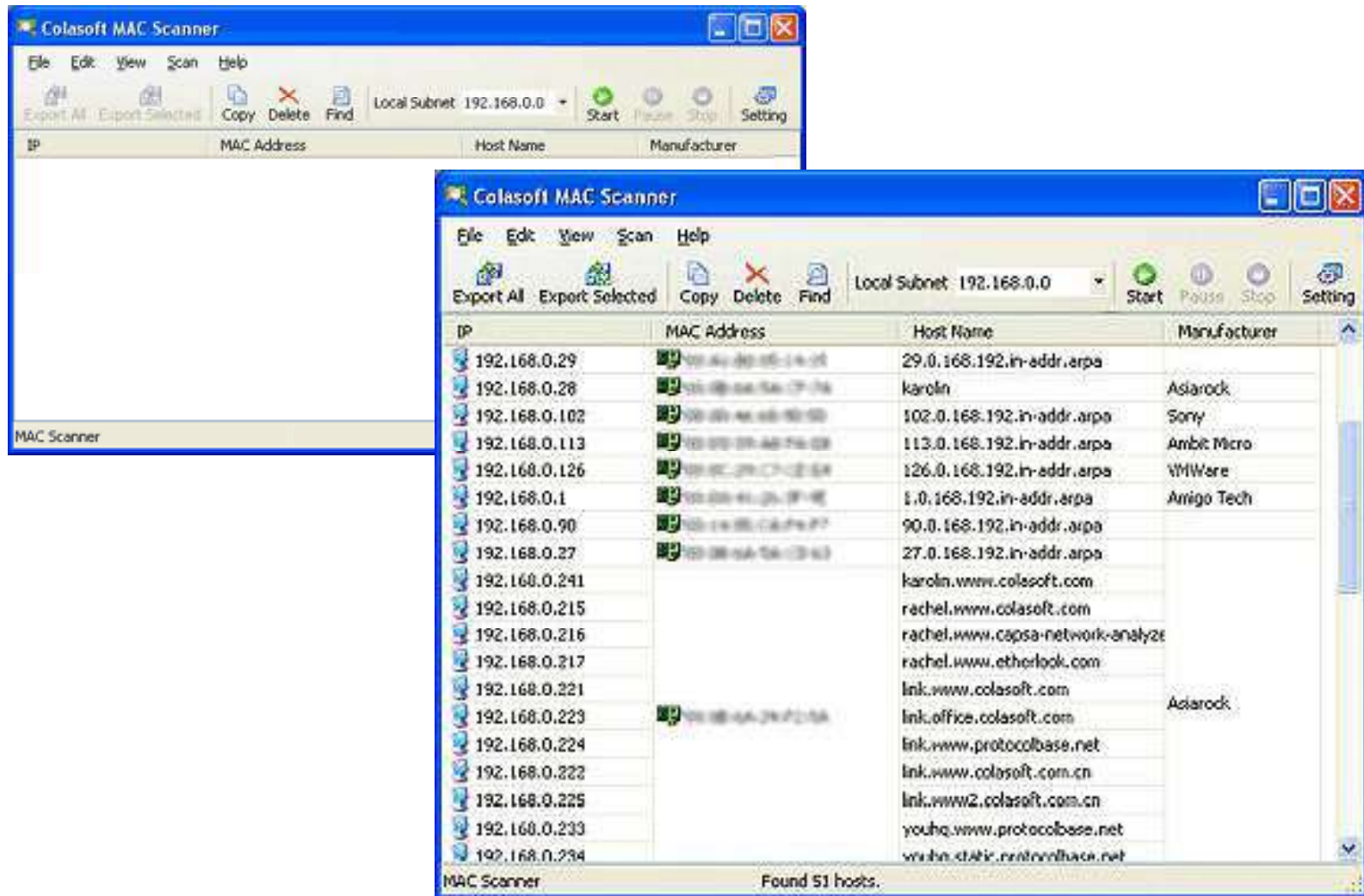
Colasoft MAC scanner allows to scan the network and get a list of MAC addresses along with IP address, machine name, and manufacturer's information

It can automatically detect all subnets according to the IP addresses configured on multiple NICs of a machine

It supports multi-threaded scanning



# Colasoft MAC Scanner: Screenshot



# Active Network Monitor

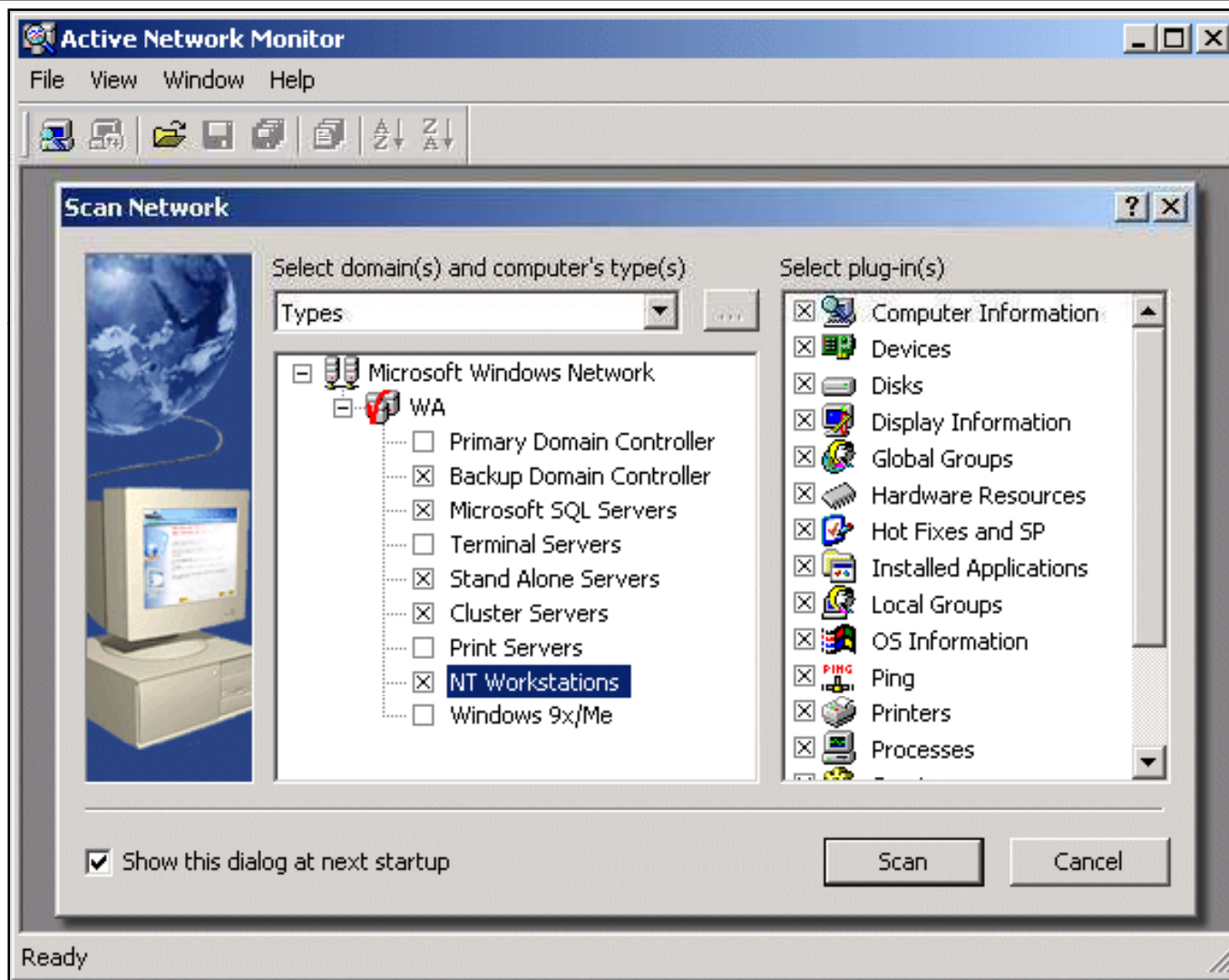
Active Network Monitor allows Systems Administrators to gather information from all machines in the network without installing server-side applications on these computers

Allows to view, store, and compare the received data

Selects a variety of items to be scanned, including installed applications, hotfixes, hardware resources, OS information, and computer information

Results are in-depth; however, they are displayed in individual windows for each scan and can be hard to manage if many items are included

# Active Network Monitor: Screenshot



# Advanced Serial Data Logger

Advanced Serial Data Logger is a serial port data logging and monitoring solution that can be used as serial port and RS232 real time sniffer or to log all received data to a local file

It captures serial data, custom tailors it to your needs, then extracts bits of data from data packets, and transfers the data to any Windows or DOS application

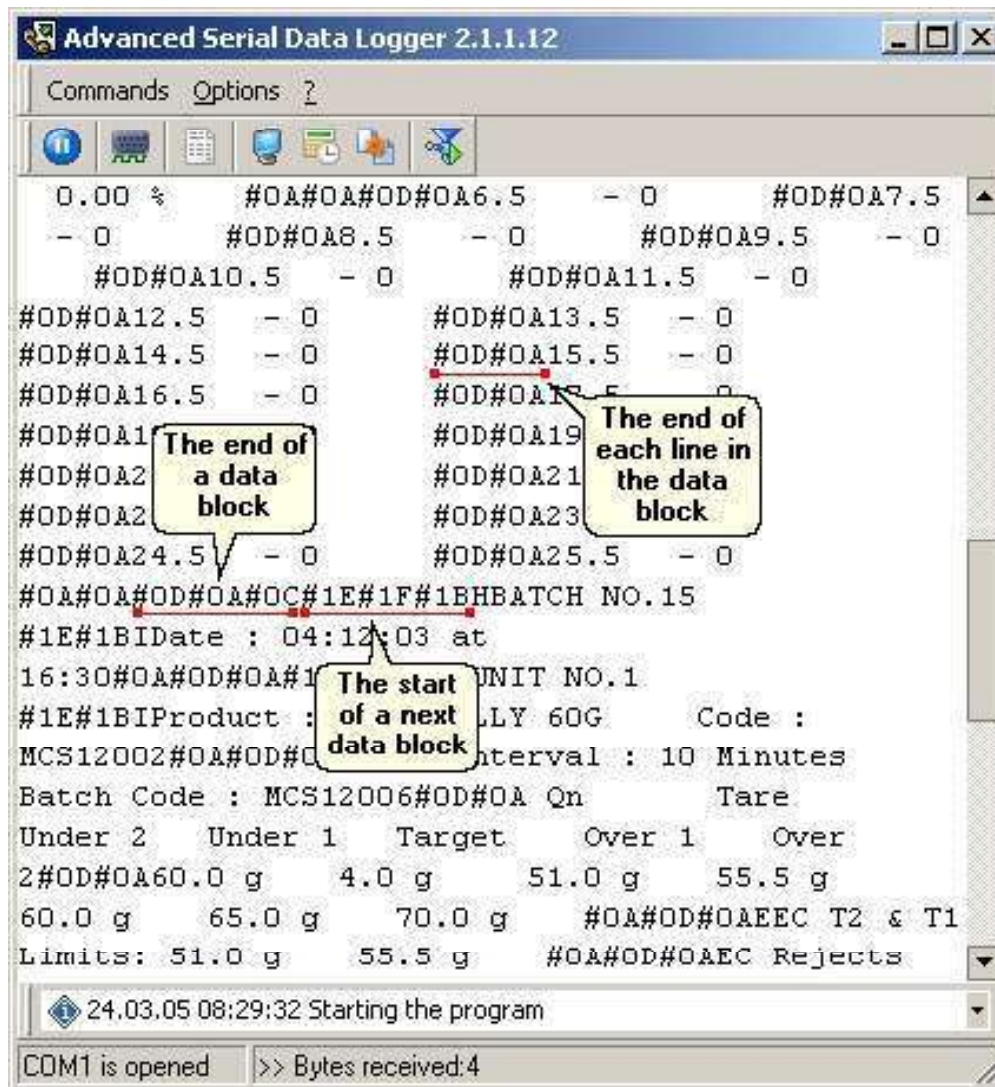
It captures data either by sending keystrokes to the application window, or by passing the data through Dynamic Data Exchange conversations, ODBC, OLE

It supports RS-485, full duplex mode, flexible parameters, plug-ins, and can run as a service

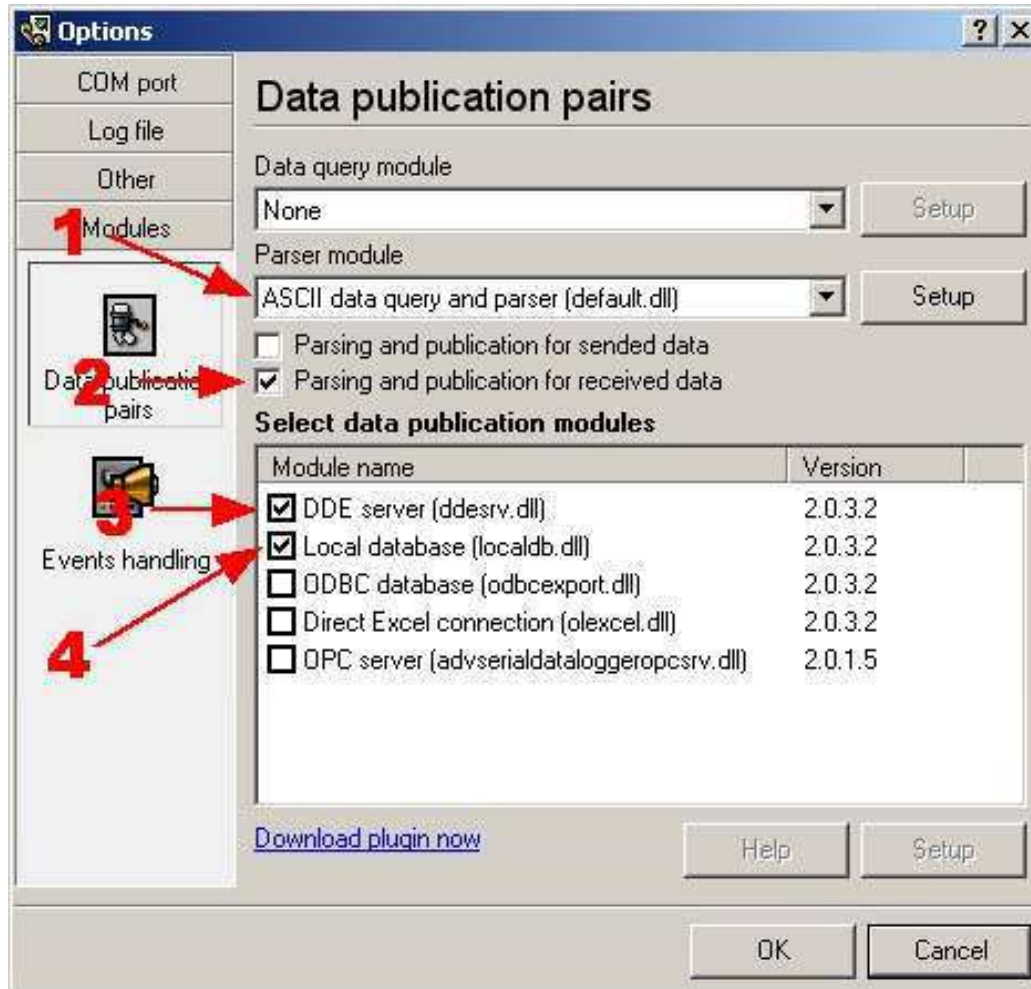
It also transmits requests or commands out the serial port to control or query your instruments directly from Advanced Serial Data Logger over ASCII or MODBUS protocol



# Advanced Serial Data Logger: Screenshot 1



# Advanced Serial Data Logger: Screenshot 2





# Advanced Serial Port Monitor

This program allows to check the flow of data through a computer's COM ports

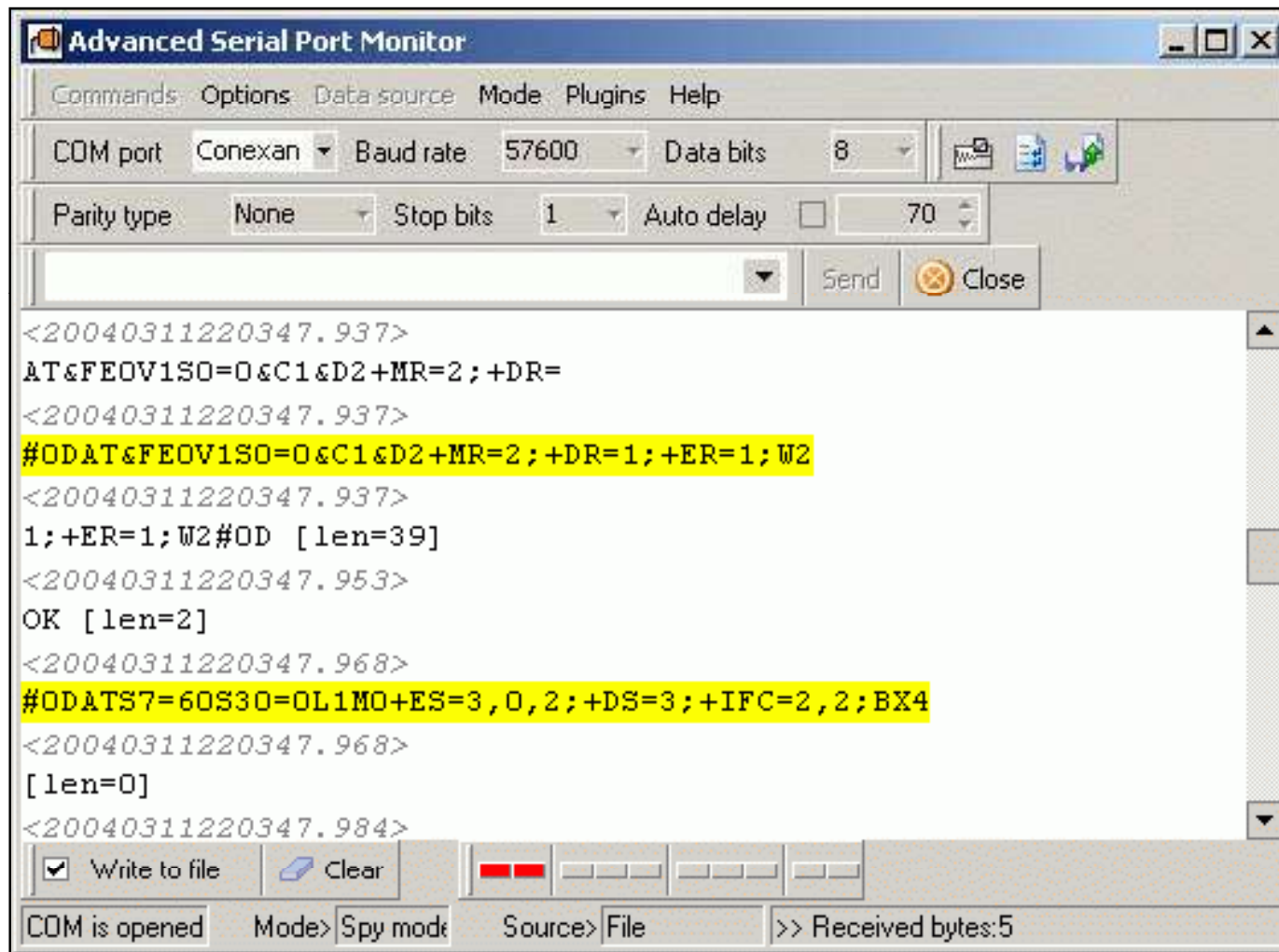
It can work as serial port monitor and supports full duplex mode, output received data to file, free data source, and serial device simulation

It supports the miscellaneous baudrates (up to 115200), number of databits, number of stop bits, different types to parity, flow control types and others

It can monitor the data exchange between any external devices, connected to serial port and Windows applications

It can run with predefined options and actions or execute commands from plugins

# Advanced Serial Port Monitor: Screenshot





WotWeb is a port scanner specifically made to scan and display active web servers and shows the server software running on them

IP lists can be entered manually or by reading from a file

Scanning is fast and accurate and the acquired list of servers can be saved to a comma separated text file for importing into your favorite spreadsheet application for further analysis

WotWeb was written to aid system administrators who manage large networks and need to keep track of all their web servers and the type of server software running on them

# WotWeb: Screenshot

wotweb 1.06 - Robin Keir - keir.net

**IPs**

Hostname/IP: 192.168.1.5

Start IP: 192 . 168 . 1 . 1

End IP: 192 . 168 . 1 . 10

Read IPs from file: Browse...

Start IP	End IP
192.168.1.1	192.168.1.10

Clear Selected  
Clear All

**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 type="checkbox"/> 8080	<input type="checkbox"/> 9090
<input checked="" type="checkbox"/> 443	<input type="checkbox"/> 2779	<input type="checkbox"/> 6588	<input 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
192.168.1.1	80	401	Basic	[Unknown]
192.168.1.3	80	400	None	Powered By IISShield/1.0 (KodelT)

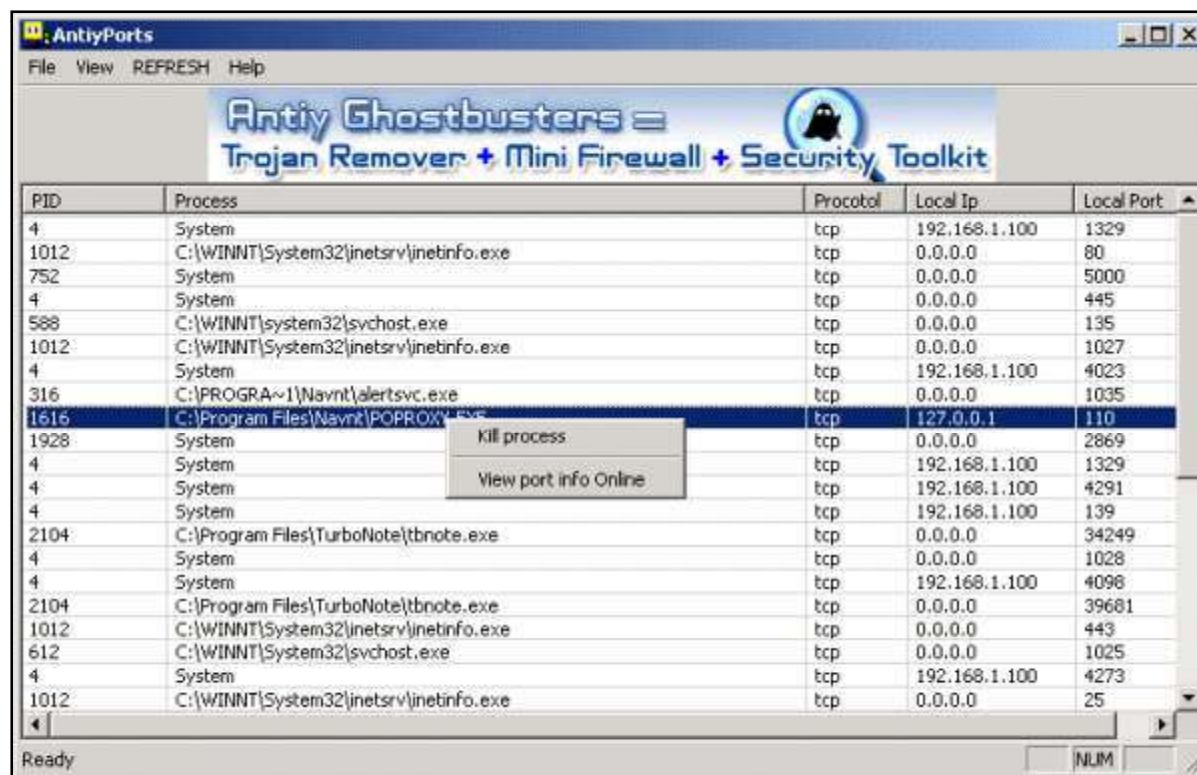
Ports scanned: 20/20

Save...

# Antiy Ports

Antiy Ports is a TCP/UDP port monitor that maps the ports in use to the applications that are currently using them

It offers to kill any selected process and links to additional port information online



# Port Detective

Port Detective is a tool that helps you find out what ports are blocked by the router, firewall, or ISP

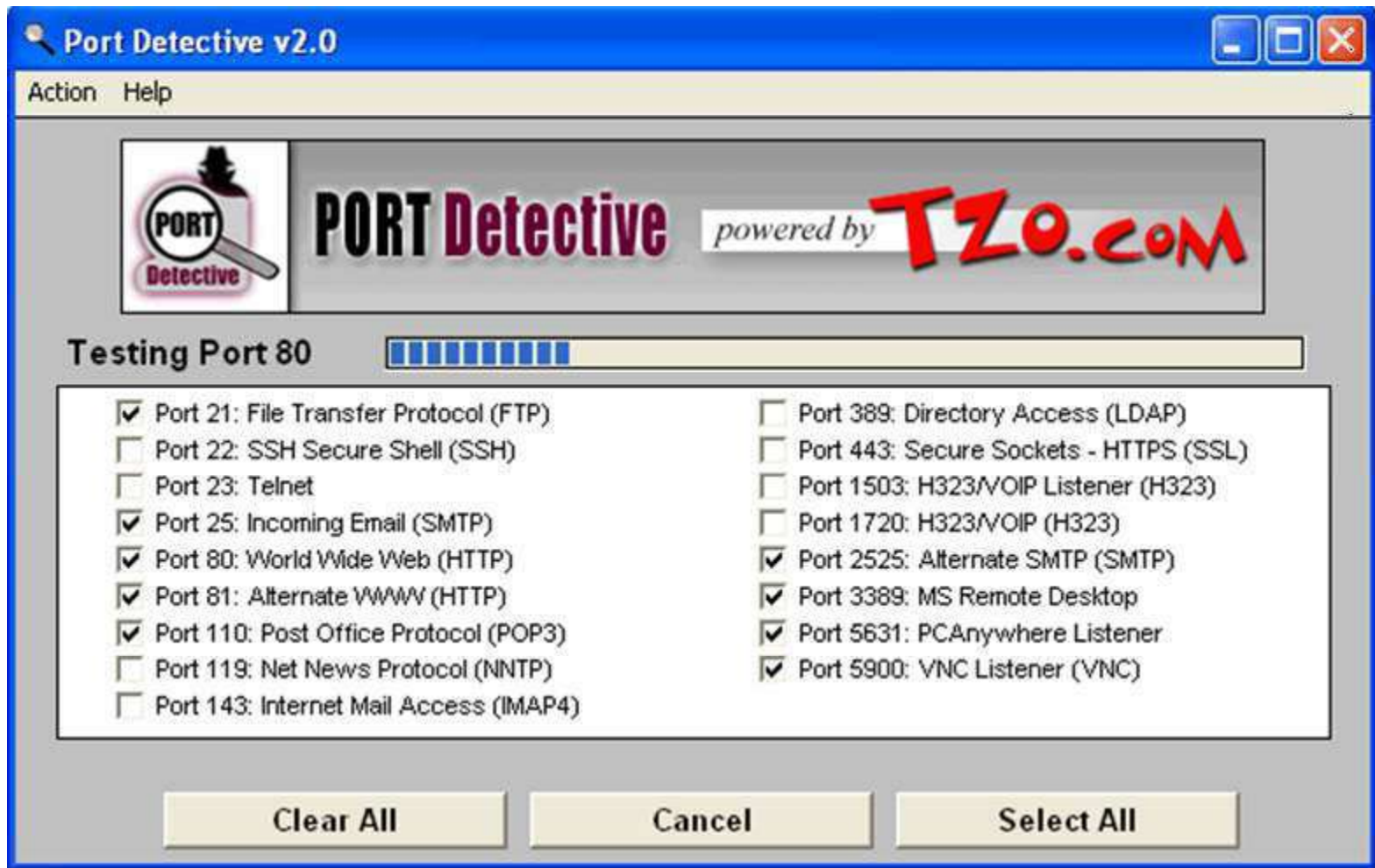


It comes pre-configured for the most commonly used ports, and you can also add your own ports to the list

The program is intended to check the availability of common ports for the purpose of self-hosting, as many ISPs are blocking these ports to prevent users from running public web servers, mail servers etc. on their home computers



# Port Detective: Screenshot







Roadkil's Detector is a simple port listener, that allows to monitor connections to the specific system ports

It displays the IP address of the connecting agent, the remote machine's name, as well as time and date of the connection

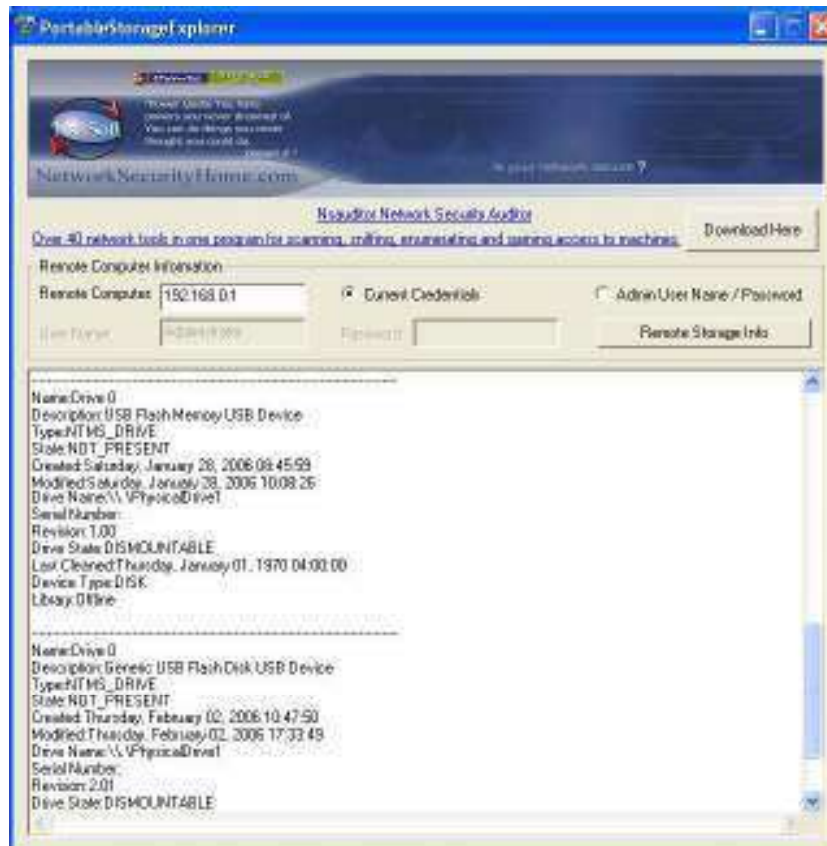
The output can optionally be saved to a log file





# Portable Storage Explorer

Portable Storage Explorer displays remote network computer USB devices, removable storage, CD-Rom and DVD drive information and state, drive type, serial number, revision, device name, last cleaned time, device vendor and product name, operational state, created and modified time, device library, etc





# War Dialer Technique

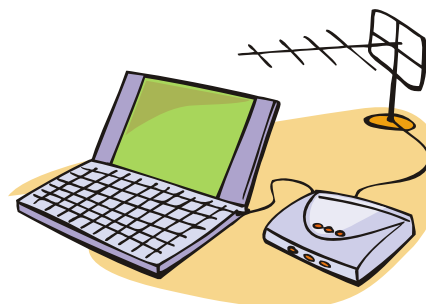
# War Dialer Technique

War dialing involves the use of a program in conjunction with a modem to penetrate the modem-based systems of an organization by continually dialing in

Companies do not control the dial-in ports as strictly as the firewall and machines with modems attached are present everywhere

A tool that identifies the phone numbers that can successfully make a connection with a computer modem

It generally works by using a predetermined list of common user names and passwords in an attempt to gain access to the system



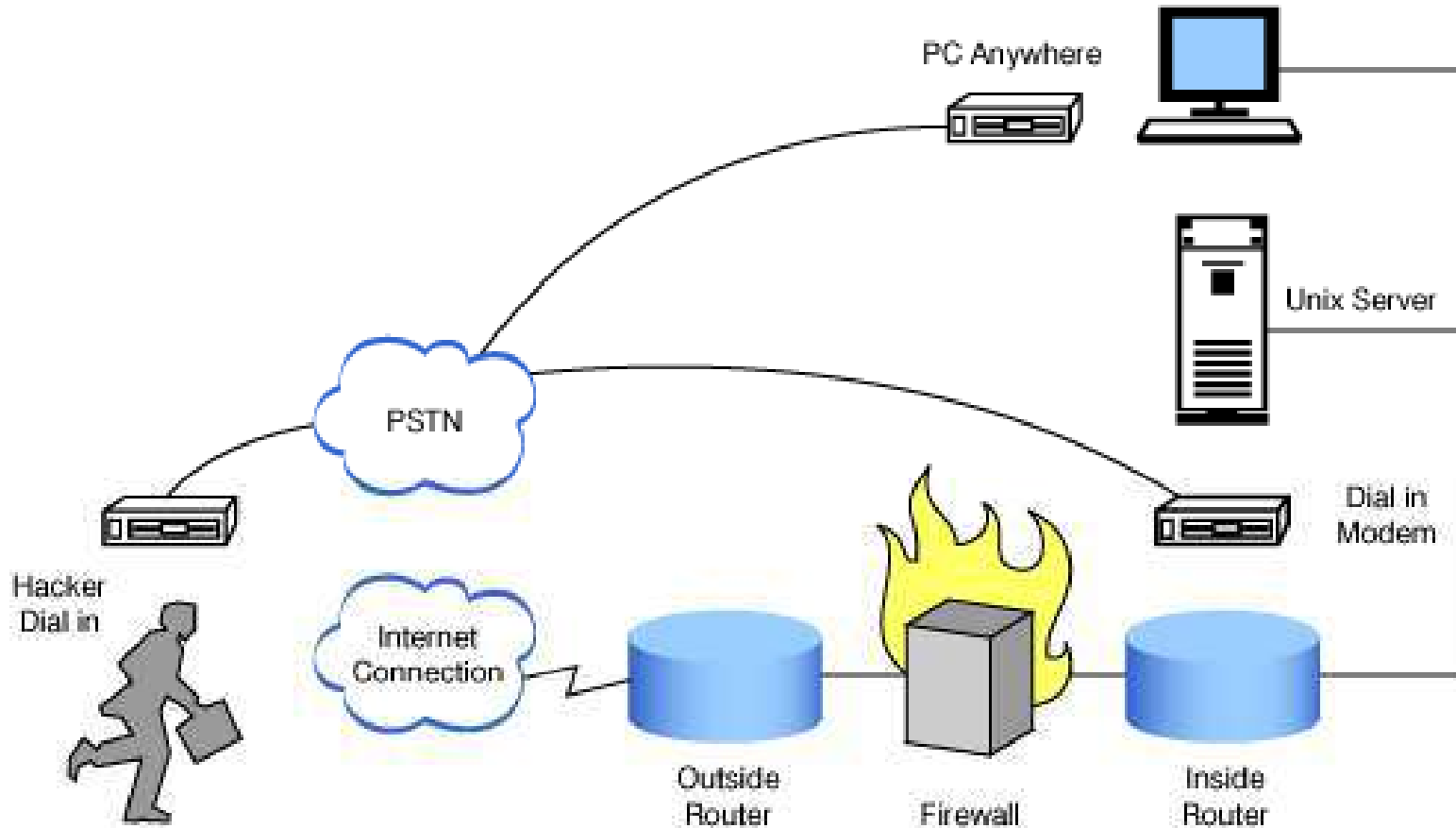
# Why War Dialing?

*It doesn't matter how strongly you've locked the front door to your network if you've left the back door wide open*

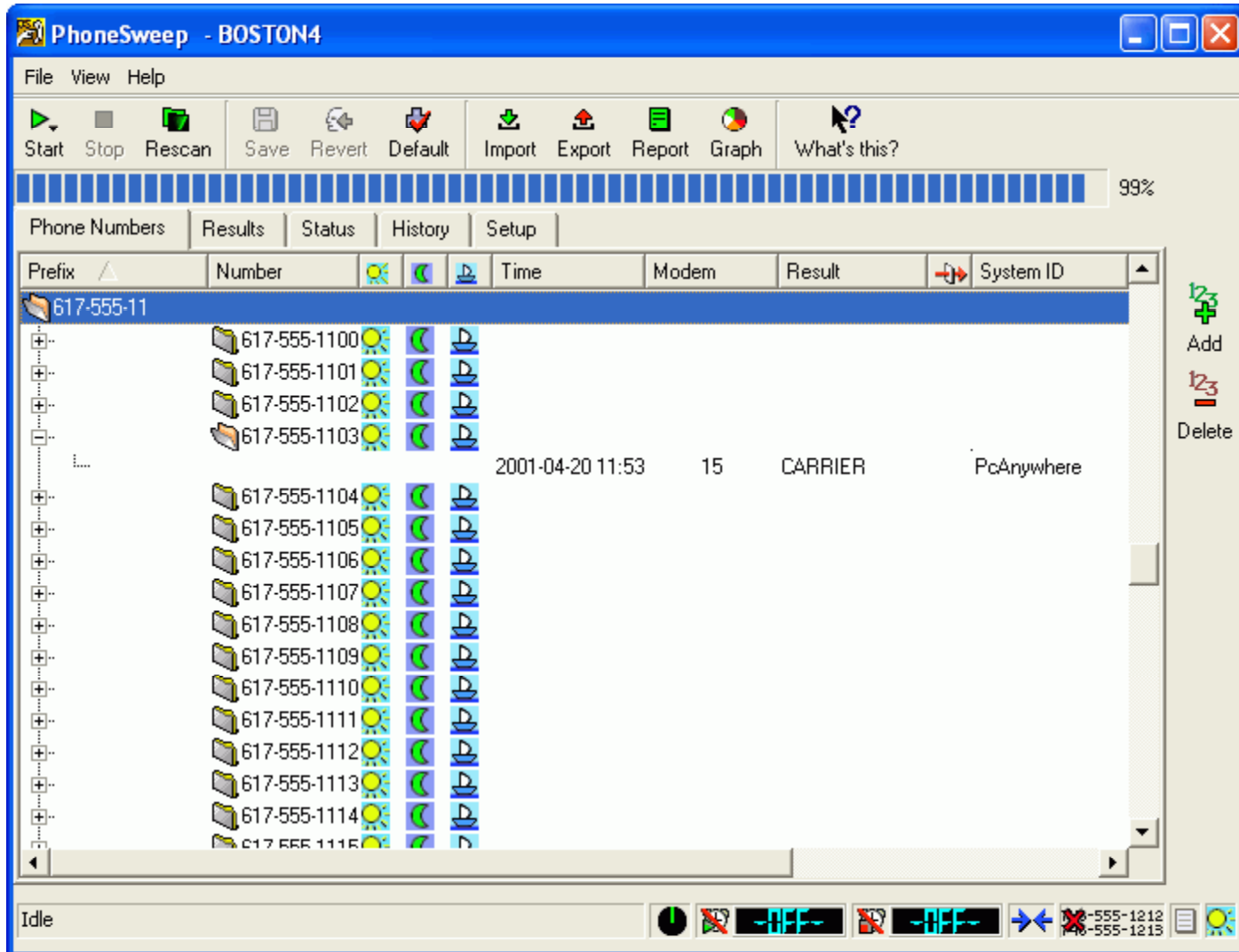
- Has someone inside your organization attached a modem to your network?
- Are your authorized modems susceptible to a break-in with a wardialer?
- Are your modems revealing banners with their identity?
- Do your modems still have default manufacturer passwords?
- Is there unknown open access to a legacy system?
- Are you at risk by not conducting regular audits across your organization?



# Wardialing



# PhoneSweep – War Dialing Tool



```
Scan Mode : CARRIERS
Dial Mode : RANDOM
Manual/Autonom Mode : OFF
Step Rate : 0
Manual Timeout : 30
CARRIER Hack Mode : NUDGE
Nudge Delay : 60
Nudge : ~~~~~M?M help M guest M guest M INFO M MLO
Timeout : 50 seconds
Ringout : 6 seconds
Redial Busy : YES
BUSY Overwrite : NO
Calculate Elapsed Time : YES
NO DIALTONE exit : 20
Auto DAI save time : 10 minutes
DATA save exceptions : 0
DAI Filename calculation : Delete Left + Delete Special
```

It is a type of War Dialer that scans a defined range of phone numbers

Another tool for wardialing is PhoneSweeper



ToneLoc is a popular war dialing computer program for MS-DOS

It dials numbers to look for some kind of tone

Command line options for ToneLoc:

```
ToneLoc [DataFile] /M:[Mask] /R:[Range] /D:[ExRange] /X:[ExMask]  
/C:[Config] /S:[StartTime] /E:[EndTime] /H:[Hours] /T[-] /K[-]
```

It is used to:

- Find PBX's
- Find loops or milliwatt test numbers
- Find dial-up long distance carriers
- Find any number that gives a constant tone, or something that your modem will recognize as one
- Finding carriers (other modems)
- Hacking PBX's

ModemScan is a GUI wardialer software program which utilizes Microsoft Windows Telephony

## Features:

- ModemScan works with hardware you already own and does not require the additional purchase of specific nor specialized hardware
- Randomly selects and dials phone numbers from the dial ranges list to prevent line termination from phone companies which detect sequential dialing
- Runs multiple ModemScan copies with more than one phone line and modem on the same computer
- Imports comma delimited text files containing phone numbers or ranges
- Flexible phone number dialing
- Utilizes Microsoft's Telephony settings for easy modem and location setup



# War Dialing Countermeasures SandTrap Tool

Sandtrap can detect war dialing attempts and notify the administrator immediately upon being called, or upon being connected to, via an email message, pager or via HTTP POST to a web server



```
File View Tools Help
13:38:21.5 (Fri) OS is Windows XP Service Pack 2
13:38:21.5 (Fri) ALERT: This is a Demo Version of the Sandtrap war/dialer detector. It is fully functional and
will run for 5 minutes. For more information, visit http://www.sandstorm.net. To purchase a retail version,
call Sandstorm Enterprises at +1-781-333-3000 or send e-mail to sales@sandstorm.net.
13:38:23.0 (Fri) Memory in use: 37392384
13:38:23.0 (Fri) Mapping modem 1 to port COM1
13:38:23.0 (Fri) Mapping modem 2 to port COM2
13:38:23.0 (Fri) Mapping modem 3 to port COM3
13:38:23.0 (Fri) Mapping modem 4 to port COM4
```

Conditions that can be configured to generate notification messages include:

- Incoming Caller ID
- Login attempt





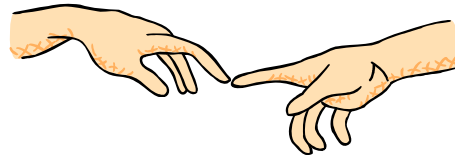
# Banner Grabbing

# OS Fingerprinting

OS fingerprinting is the method to determine the operating system that is running on the target system

The two different types of fingerprinting are:

- Active stack fingerprinting
- Passive fingerprinting



# Active Stack Fingerprinting

Based on the fact that OS vendors implement the TCP stack differently

Specially crafted packets are sent to remote OSs and the response is noted

The responses are then compared with a database to determine the OS

The Firewall logs your active banner grabbing scan since you are probing directly



# Passive Fingerprinting

Passive banner grabbing refers to indirectly scanning a system to reveal its server's operating system

It is also based on the differential implantation of the stack and the various ways an OS responds to it

It uses sniffing techniques instead of the scanning techniques

It is less accurate than active fingerprinting

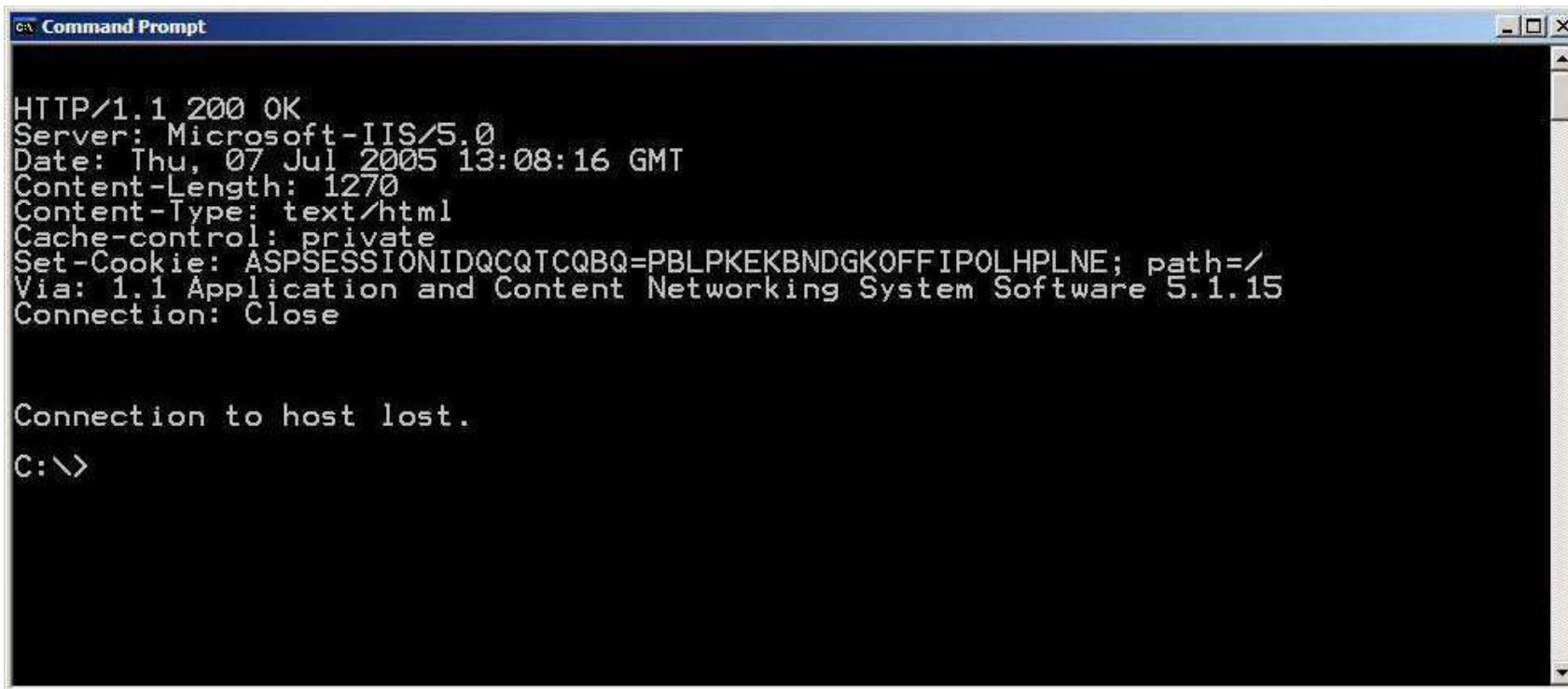




# Active Banner Grabbing Using Telnet

You can use telnet to grab the banner of a website

```
telnet www.certifiedhacker 80 HEAD / HTTP/1.0
```



```
CA Command Prompt

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 07 Jul 2005 13:08:16 GMT
Content-Length: 1270
Content-Type: text/html
Cache-control: private
Set-Cookie: ASPSESSIONIDQCQTCQBQ=PBLPKEKBNDGKOFFIPOLHPLNE; path=/
Via: 1.1 Application and Content Networking System Software 5.1.15
Connection: Close

Connection to host lost.
C:\>
```

# GET REQUESTS

You might want to try these additional get requests for banner grabbing

Take a look at :  
[GET REQUESTS KNOWN\\_TESTS.htm file](#)

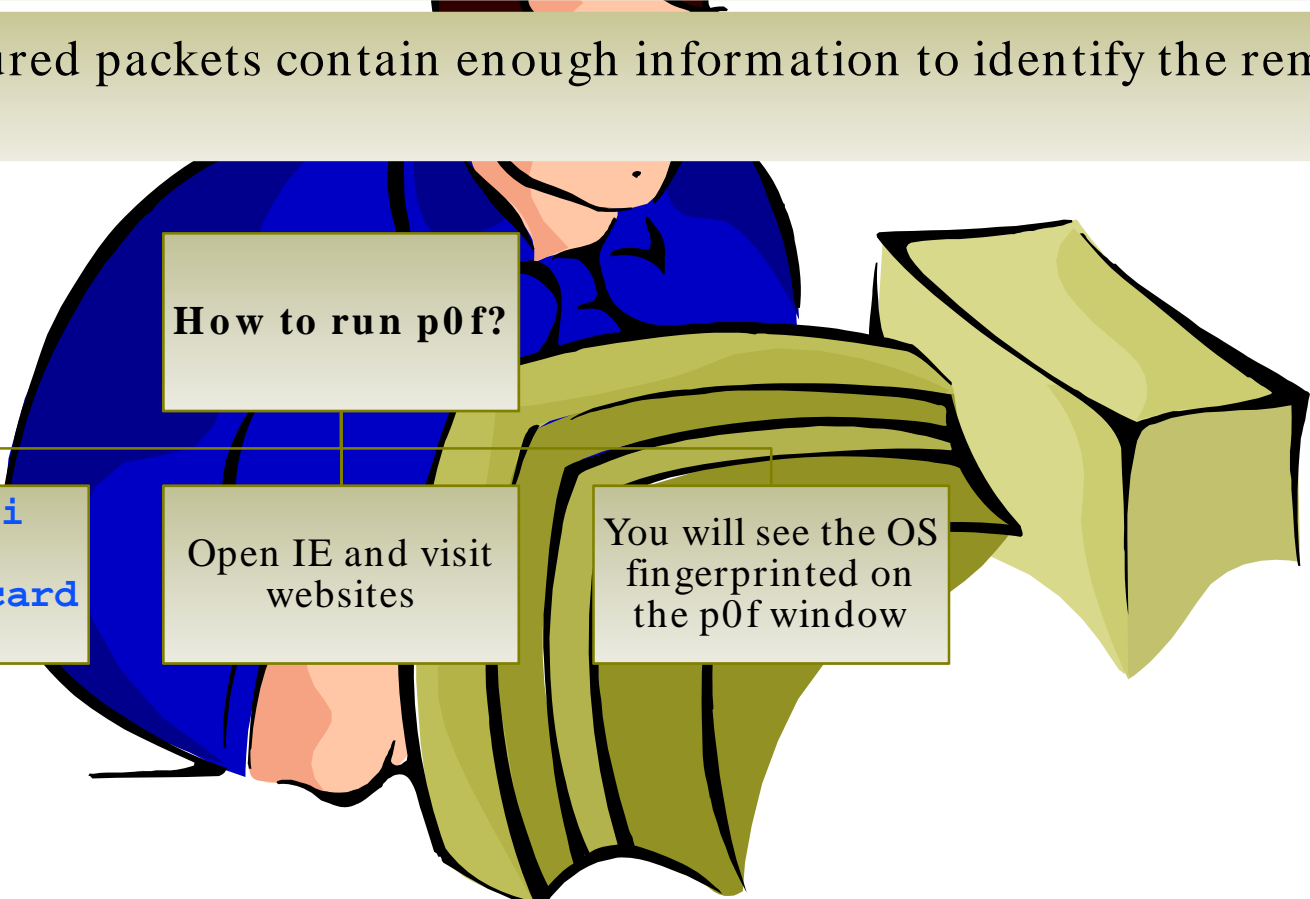


```
'GET / HTTP/1.0',
'GET / HTTP/1.0',
'GET / HTTP/999.99',
'GET / http/999.99',
'GET / http/999.99',
'GET / HTTP/Q.9',
'GET / HTTP/9.Q',
'GET / HTTP/Q.Q',
'GET / HTTP/1.X',
'GET / HTTP/1.10',
'GET / HTTP/1.1.0',
'GET / HTTP/1.2',
'GET / HTTP/2.1',
'GET / HTTP/1,0',
'GET / HTTP/1.OX',
'GET / HTTP/',
'GET/HTTP/1.0 ',
'GET/ HTTP/1.0 ',
'GET /HTTP/1.0 ',
'GET/HTTP /1.0 ',
'GET/HTTP/1 .0 ',
'GET/HTTP/1. 0 ',
'GET/HTTP/1.0 ',
'GET / HTTP /1.0',
'HEAD /.\\ HTTP/1.0',
'HEAD /asdfasdfasdfasdf/.. HTTP/1.0',
'HEAD /asdfasdfasdfasdf/.. HTTP/1.0',
'HEAD /./././././././././././././././ HTTP/1.0',
'HEAD /./././././././././././././././ HTTP/1.0',
'HEAD /.. HTTP/1.0',
'HEAD /./ HTTP/1.0',
'HEAD /./ HTTP/1.0',
'HEAD / HTTP/1.0',
'HEAD \t\cHTTP/1.0',
'HEAD // HTTP/1.0',
'Head / HTTP/1.0',
'\nHEAD / HTTP/1.0',
' \nHEAD / HTTP/1.0',
' HEAD / HTTP/1.0',
'HEAD / HQWERTY/1.0',
'HEAD %s HTTP/1.0' % url,
'HEAD %s' % url,
'HEAD http:// HTTP/1.0',
'HEAD http:// HTTP/1.0',
'HEAD http: HTTP/1.0',
'HEAD http HTTP/1.0',
'HEAD h HTTP/1.0',
'HEAD HTTP://qwerty.asdfg.com/ HTTP/1.0',
'GET GET GET',
'HELLO',
' GET / HTTP/1.0',
' '*1000 + 'GET / HTTP/1.0',
'GET'+ ' '*1000+' HTTP/1.0',
'GET '+'/'*1000+' HTTP/1.0',
'GET /'+ ' '*1000+'HTTP/1.0',
'GET / '+H'*1000+'TTP/1.0',
'GET / '+HTTP'+/'*1000+'1.0',
'GET / '+HTTP/'+1'*1000+'0',
'GET / '+HTTP/1+'.'*1000+'0',
'GET / '+HTTP/1.'+0'*1000,
'GET / HTTP/1.0' + ' ' * 1000,
'12345 GET / HTTP/1.0',
'12345 / HTTP/1.0',
'\0',#70
'\0'*1000,
'\0'+GET / HTTP/1.0',
'\0'*1000+'GET / HTTP/1.0',
'\r\n'*1000+'GET / HTTP/1.0',
'Get / HTTP/1.0',
'GET\0\0HTTP/1.0',
'GET . HTTP/1.0',
'GET index.html HTTP/1.0',
'GET / HTTP/1.',
'',
'',
' '*1000,
'',
' '*1000,
'GET FTP://asdfasdf HTTP/1.0',
'GET / HTTP/1.0 X',
'%47ET / HTTP/1.0',
'%47%45%54 / HTTP/1.0',
'GET %2f HTTP/1.0',
'GET %2F HTTP/1.0',
'GET%20/ HTTP/1.0',
'GET / FTP/1.0',
'GET \ HTTP/1.0',
'GET C:\ HTTP/1.0',
'HTTP/1.0 / GET',
'ALL YOUR BASE ARE BELONG TO US',
'GET "/" HTTP/1.0',
'GET '/' HTTP/1.0',
'GET ` ` HTTP/1.0',
'"GET / HTTP/1.0"',
'"GET / HTTP/1.0',
'"GET" / HTTP/1.0',
'"'GET / HTTP/1.0',
'GEX\bT / HTTP/1.0',
```

# p0f – Banner Grabbing Tool

p0f is a passive OS fingerprinting technique that is based on analyzing the information sent by a remote host

The captured packets contain enough information to identify the remote OS



How to run p0f?

Run `p0f -i`  
`<your`  
`interface card`  
`number>`

Open IE and visit  
websites

You will see the OS  
fingerprinted on  
the p0f window

# p0f for Windows

EC-Council University - Windows Internet Explorer

```
C:\WINDOWS\System32\cmd.exe
J:\Ethical Hacking and Countermeasures v5\Module 03 - Scanning\p0f>p0f -i 2
p0f - passive os fingerprinting utility, version 2.0.4
(C) M. Zalewski <lcantuf@dione.cc>, W. Stearns <wstearns@pobox.com>
WIN32 port (C) M. Davis <mike@datanerds.net>, K. Kuehl <kkuehl@cisco.com>
p0f: listening (SYN) on '\Device\NPF_{CCA17F4E-51D5-4A9F-918B-F59F0643E936}', 22
3 sigs (12 generic), rule: 'all'.
10.0.0.11:14638 - Windows 2000 SP4, XP SP1
-> 64.90.188.178:80 (distance 0, link: ethernet/modem)
10.0.0.11:14639 - Windows 2000 SP4, XP SP1
-> 64.90.188.178:80 (distance 0, link: ethernet/modem)
10.0.0.11:14640 - Windows 2000 SP4, XP SP1
-> 64.90.188.178:80 (distance 0, link: ethernet/modem)
10.0.0.11:14641 - Windows 2000 SP4, XP SP1
-> 64.90.188.178:80 (distance 0, link: ethernet/modem)
10.0.0.11:14642 - Windows 2000 SP4, XP SP1
-> 64.90.188.178:80 (distance 0, link: ethernet/modem)
10.0.0.11:14643 - Windows 2000 SP4, XP SP1
-> 64.90.188.178:80 (distance 0, link: ethernet/modem)
10.0.0.11:14644 - Windows 2000 SP4, XP SP1
-> 64.90.188.178:80 (distance 0, link: ethernet/modem)
10.0.0.11:14645 - Windows 2000 SP4, XP SP1
-> 64.90.188.178:80 (distance 0, link: ethernet/modem)
10.0.0.11:14646 - Windows 2000 SP4, XP SP1
-> 64.90.188.178:80 (distance 0, link: ethernet/modem)
```

1

2

- Fast - Earn your master's degree in 8-10 months.
- Relevant - Gain expertise in Business, IT, Design, or Education, four of the most in-demand fields in today's tough job market
- Effective - College graduates earn 60% more than non-college graduates. Advanced degree-holders earn almost twice the income of non-college graduates

EC-Council University is a private learning institution, offering programs at the master's degree levels in e-Business and Information Technology. Adult Students benefit from the opportunities to complete college courses and to obtain college degrees.

Privacy Statement | Copyright | Contact Us

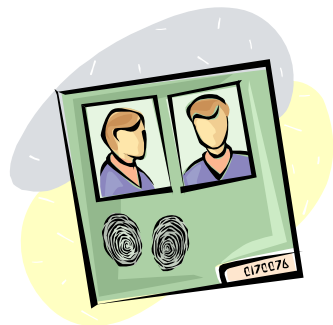
# Httpprint Banner Grabbing Tool

**httpprint** is a web server fingerprinting tool

It relies on web server characteristics to accurately identify web servers, despite the fact that they may have been obfuscated by changing the server banner strings, or by plug-ins such as mod\_security or servermask

**httpprint** can also be used to detect web-enabled devices which do not have a server banner string, such as wireless access points, routers, switches, and cable modems

**httpprint** uses text signature strings and it is very easy to add signatures to the signature database



# Httpprint: Screenshot

httpprint version 0.301

Input File: 03 - Scanning\httpprint web fingerprint\httpprint\_301\win32\input.txt

Signature File: J:\Ethical Hacking and Countermeasures v5\Module 03 - Scannin

Host	Port	Banner Reported	Banner Deduced	Conf.%
www.apache.org	80	Apache/2.2.2 (Unix)	Apache/2.0.x	78.31

Apache/2.2.2 (Unix)  
9E431BC86ED3C295811C9DC5811C9DC5050C5D32505FCFE84276E4BB811C9DC5  
0D7645B5811C9DC5811C9DC5CD37187C11DDC7D7811C9DC5811C9DC58A91CF57  
FCCC535B6ED3C295FCCC535B811C9DC5E2CE6927050C5D336ED3C295811C9DC5  
6ED3C295E2CE6926811C9DC56ED3C2956ED3C2956ED3C2956ED3C295E2CE6923  
E2CE69236ED3C295811C9DC5E2CE6927E2CE6923

Apache/2.0.x: 130 78.31  
Apache/1.3.[4-24]: 122 62.83  
Apache/1.3.[1-3]: 122 62.83  
Apache/1.3.27: 121 61.05

Report File: J:\Ethical Hacking and Countermeasures v5\Module 03 - Scannin

Report Format:  html  xml  csv

httpprint has been completed..

# Tool: Miart HTTP Header

Miart HTTP Header is a simple tool to get the HTTP Header information from any website by entering the URL into the program

It also includes:

Ping tool

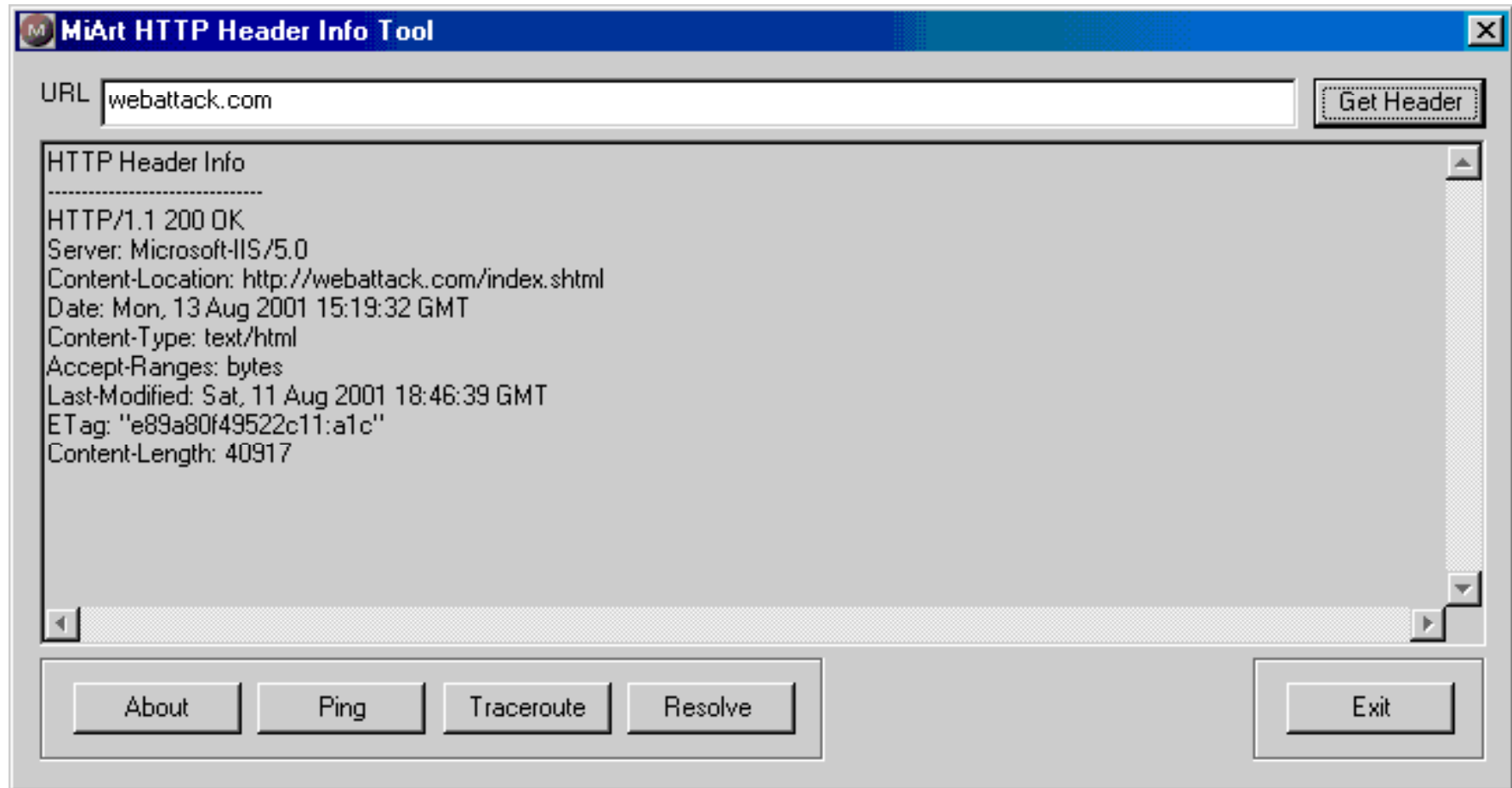
Traceroute tool

Domain name/IP resolver





# Miart HTTP Header: Screenshot



# Tools for Active Stack Fingerprinting

## XPROBE2

- It is a remote OS detection tool which determines the OS running on the target system with minimal target disturbance

## RING V2 <http://www.sys-security.com/>

- This tool is designed with a different approach to OS detection
- This tool identifies the OS of the target system with a matrix-based fingerprinting approach

Most of the port scanning tools like Nmap are used for active stack fingerprinting



Netcraft toolbar  
 (<http://www.netcraft.com>)  
 can be used to identify the  
 remote OS of a target  
 system passively



Netcraft What's That Site Running Results - Mozilla Firefox

http://ip1mw.netcraft.com/cgi/raph/site/www.italia.it

Netcraft What's That Site Running

**NETCRAFT** Secure Server Survey 24 HR BANKING

What's that site running? www.italia.it

OS, Web Server and Hosting History for www.italia.it

Try out the Netcraft Toolbar

https://www.italia.it was running Apache on Linux when last queried at 10-Mar-2007 01:18:46 GMT - refresh now Site Report

OS	Server	Last changed	IP address	NetBlock Owner
Linux	Apache/2.0.45 (Red Hat)	9-Mar-2007	129.35.116.3	Network of IBM E-business Hosting Delivery
Linux	unknown	8-Mar-2007	129.35.116.3	Network of IBM E-business Hosting Delivery
Linux	Apache/2.0.48 (Red Hat)	5-Mar-2007	129.35.116.2	Network of IBM E-business Hosting Delivery
Linux	unknown	4-Mar-2007	129.35.116.3	Network of IBM E-business Hosting Delivery
Linux	Apache/2.0.46 (Red Hat)	24-Feb-2007	129.35.116.3	Network of IBM E-business Hosting Delivery
unknown	Apache/2.0.46 (Red Hat)	23-Feb-2007	129.35.116.3	Network of IBM E-business Hosting Delivery
Linux	Apache/2.0.46 (Red Hat)	14-Feb-2007	129.35.116.3	Network of IBM E-business Hosting Delivery
Linux	Apache/2.0.46 (Red Hat)	15-Jan-2007	129.35.116.3	Network of IBM E-business Hosting Delivery
Linux	Apache/2.0.46 (Red Hat)	15-Jan-2007	129.35.116.3	Network of IBM E-business Hosting Delivery
unknown	Apache/2.0.48 (Red Hat)	18-Jan-2007	129.35.116.3	Network of IBM E-business Hosting Delivery

No uptime is currently available for www.italia.it.

Netcraft 2007

# Disabling or Changing Banner

## Apache Server

- Apache 2.x users who have the `mod_headers` module loaded can use a simple directive in their `httpd.conf` file to change banner information **Header set Server "New Server Name"**
- Apache 1.3.x users have to edit defines in `httpd.h` and recompile Apache to get the same result

IIS Server

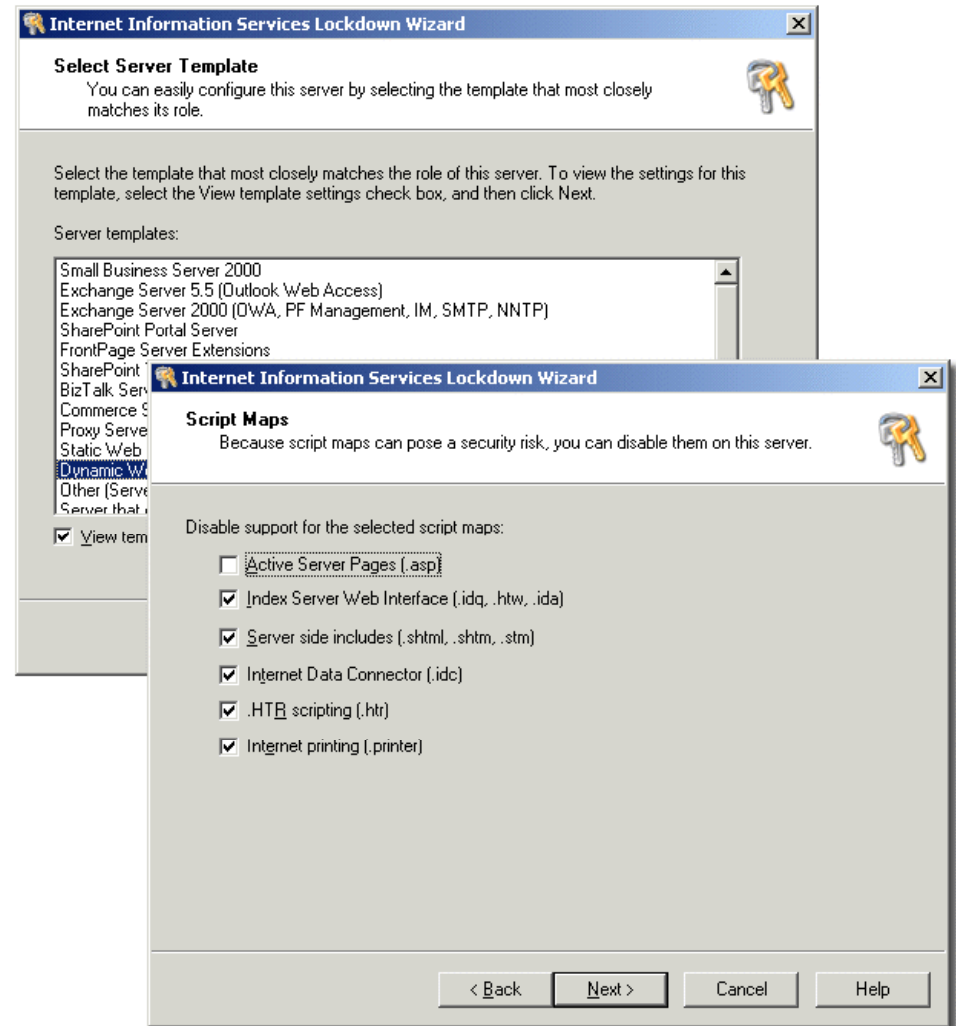
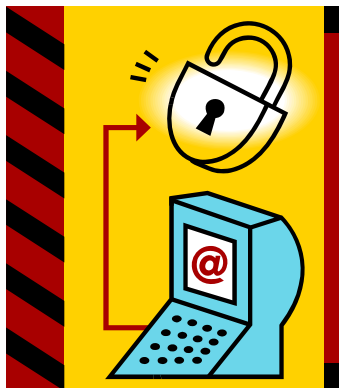
IIS users can use following tools to disable or change banner information

IIS Lockdown Tool

ServerMask

# IIS Lockdown Tool

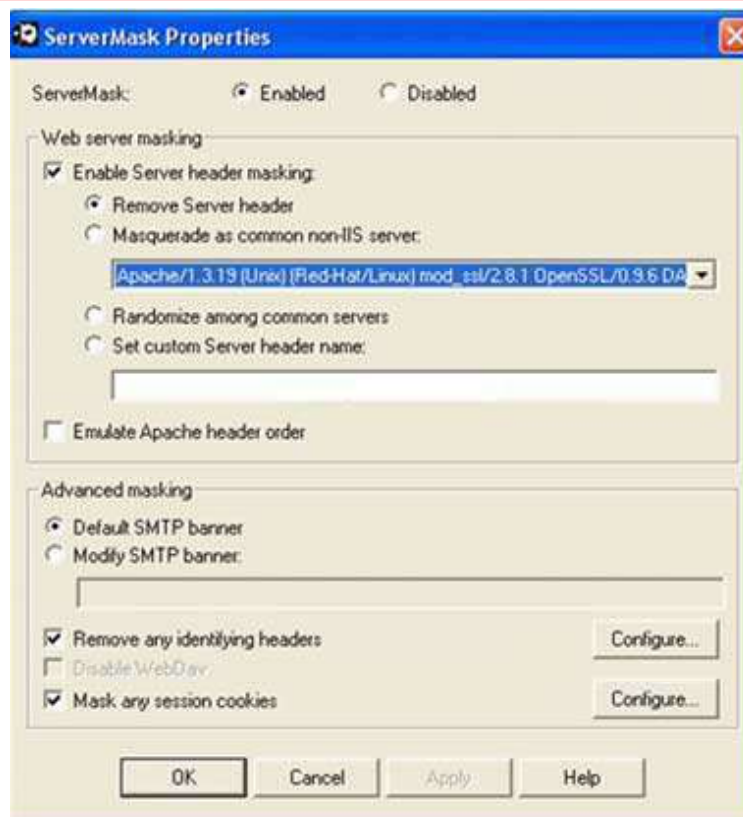
IIS Lockdown Wizard is used to turn off unnecessary features to reduce attack surface available to attackers



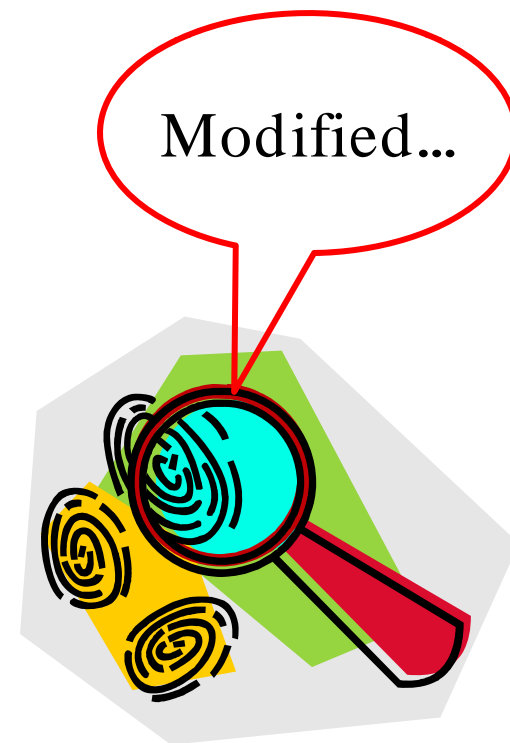
# Tool: ServerMask

It modifies web server's "fingerprint" by removing unnecessary HTTP response data, modifying cookie values and adjusting other response information

ServerMask hides the identity of server



Modified...



## Features:

- Numerous HTTP masking options
- Unique cookie masking feature
- Disables potentially dangerous features like Microsoft WebDav with one click (Windows 2000 SP3 or greater only)
- Controls other signatures such as the SMTP bannerdisplay
- Compatible with IIS Lockdown, URLScan, major thirdparty server-side scripting platforms like ASP, ASP.NET, ColdFusion, PHP, JSP, Perl
- Supports FrontPage publishing and Outlook Web Access
- Super-fast, stable ISAPI filter with no noticeable server performance impact
- Quick and easy installation and configuration





# Hiding File Extensions

Hiding file extensions is a good practice to mask the technology generating dynamic pages

Apache users can use [mod\\_negotiation](#) directives

IIS users can use tools as PageXchanger to manage file extensions



# Tool: PageXchanger

PageXchanger is a IIS server module that negotiates content with browsers and mask file extensions

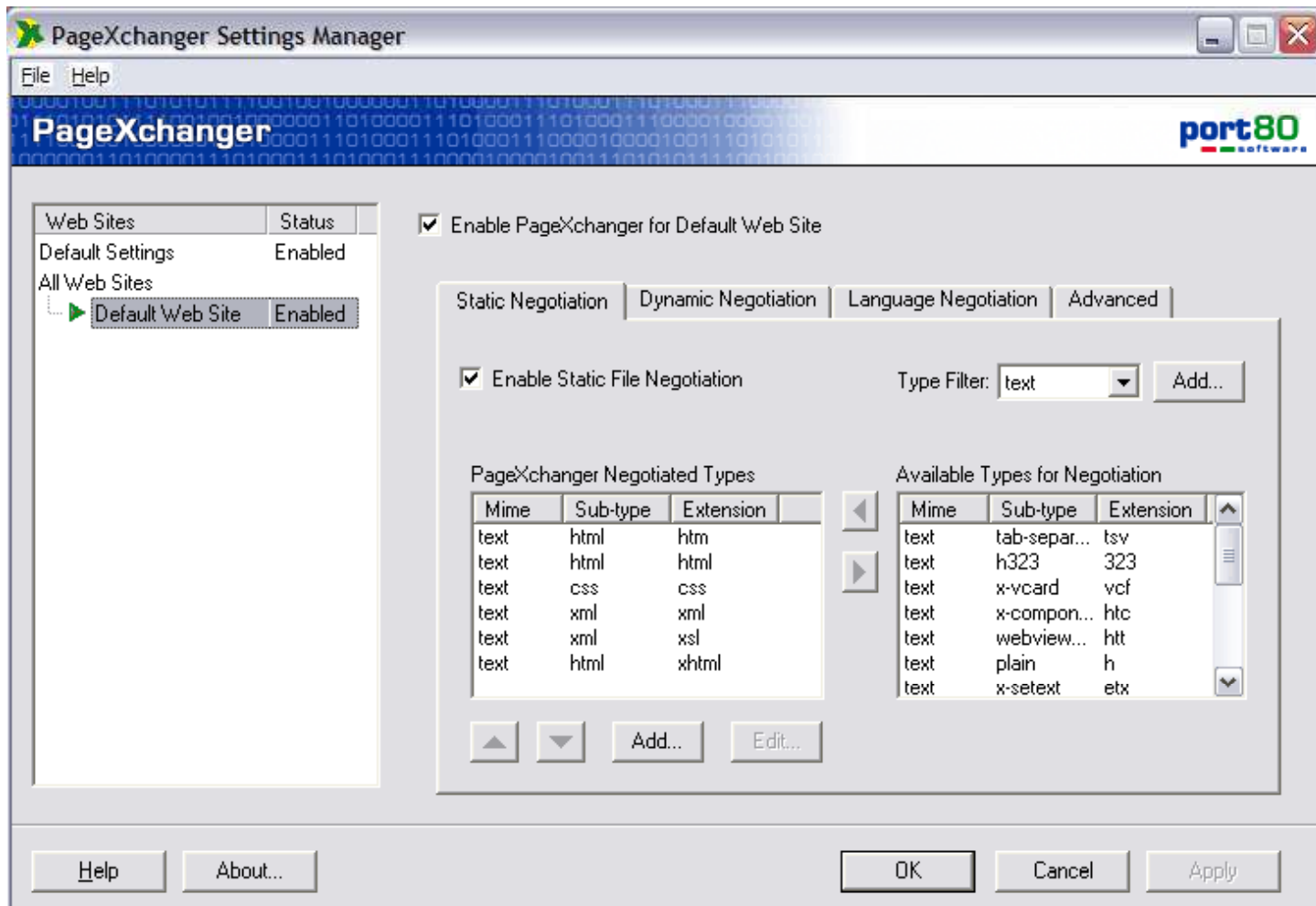
## Features:

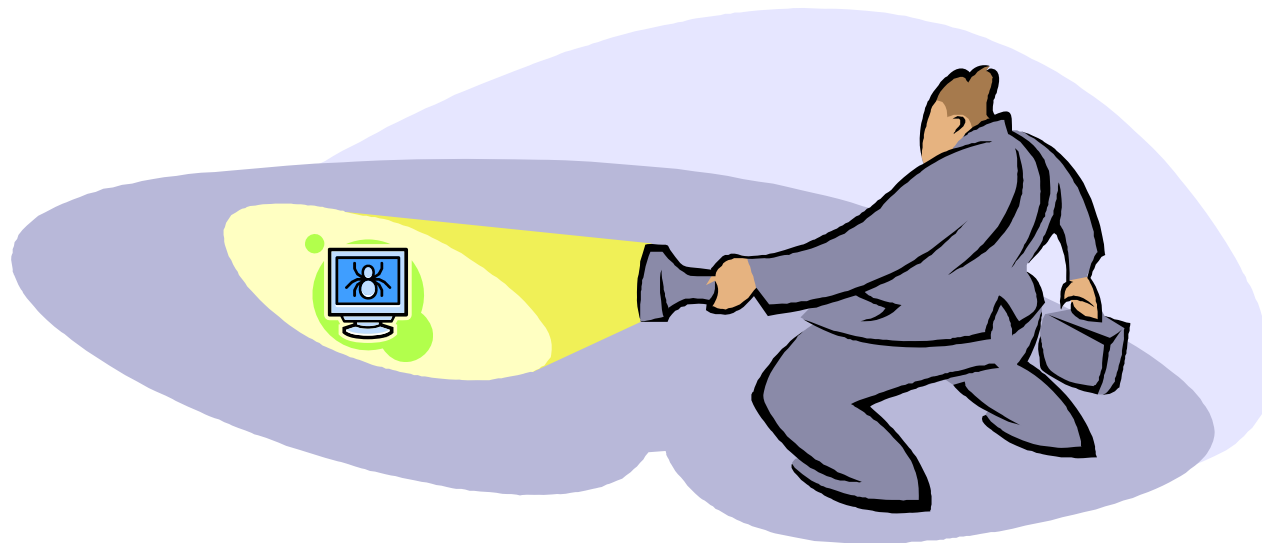
- Allows removal of file extensions in source code without affecting site functionality
- Redirects requests for pages and allows content to be served without file extensions
- URLs no longer display file extensions in a Web browser's address or location bar

## Benefits:

- Security: Enhances security by obscuring technology platform and stops hacker exploits
- Migration: Changes site technology easily without broken links or numerous redirects
- Content Negotiation: Transparently selects and serves language, image, and other content based on the user's browser
- A clean URL site: Easier for users to navigate, simple to maintain, and makes for more effective and lasting URLs in all company communications

# PageXchanger: Screenshot



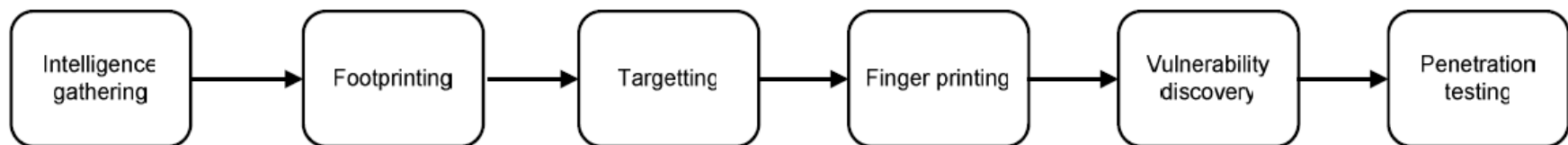


# Vulnerability Scanning

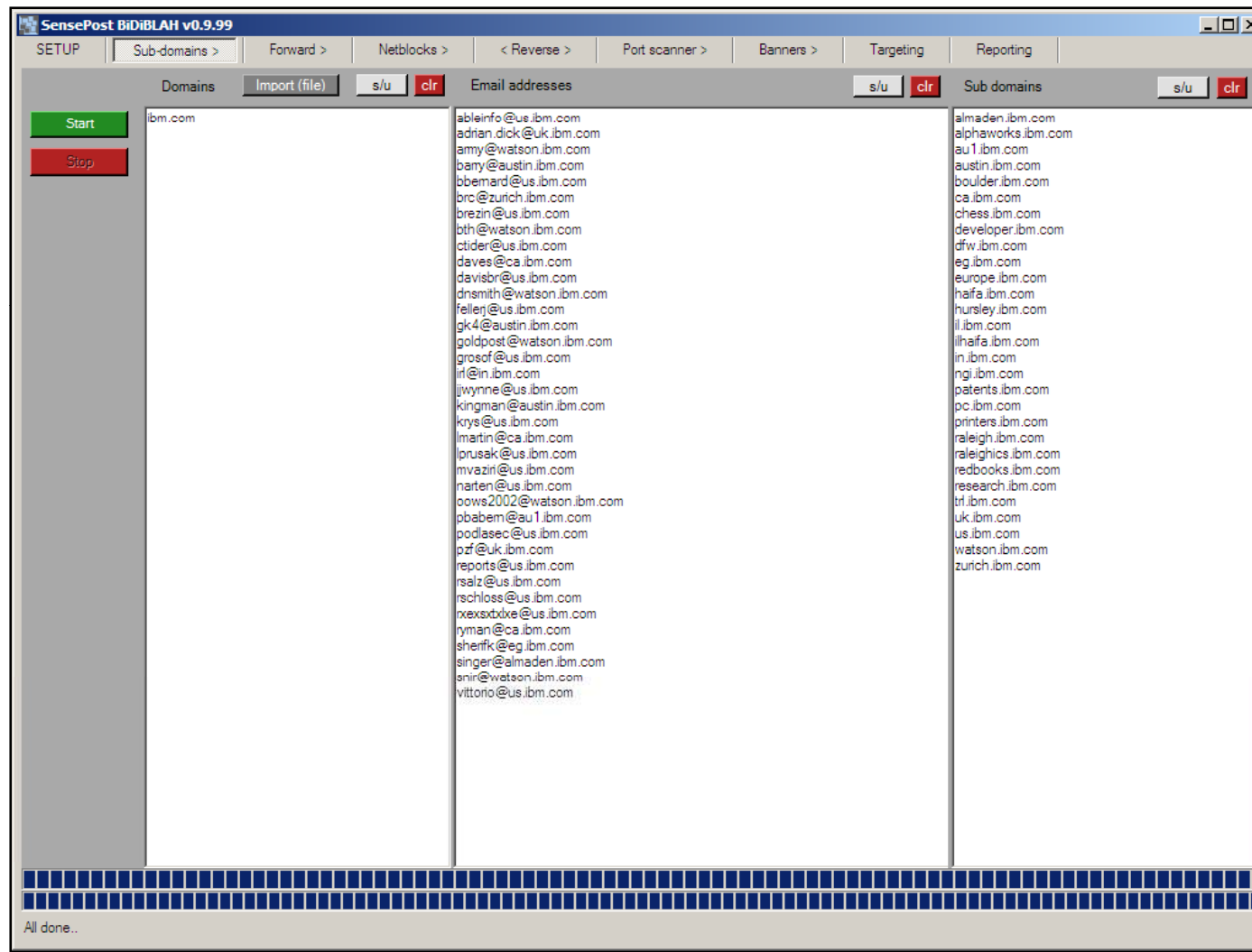
# Bidiblah Automated Scanner

Bidiblah automates footprinting, DNS enumeration, banner grabbing, port scanning, and vulnerability assessment into a single program

This tool is based on the following methodology:



# Bidiblah Automated Scanner: Screenshot





## Evaluate QualysGuard Today

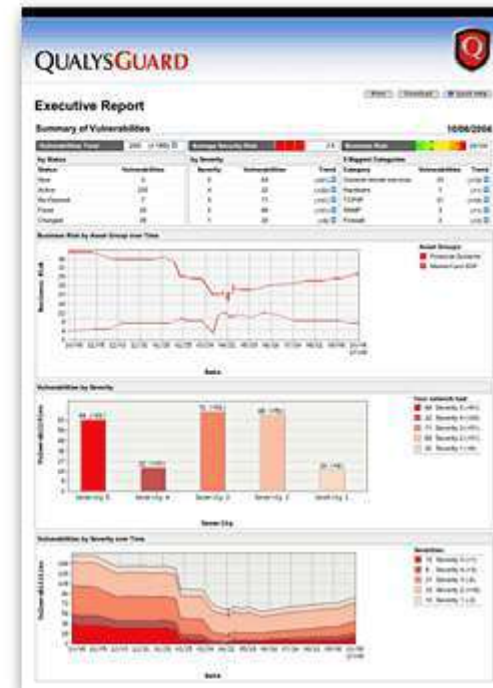
Qualys' on demand service QualysGuard provides the easiest way to manage vulnerabilities and achieve compliance. Register now for a 14-day free trial of QualysGuard and get full access to all the features that make it the most accurate and comprehensive vulnerability management solution. As an on demand service, there's no software to deploy or maintain. All you need is a Web browser, a public IP address and a few minutes to forever change the way you manage network security risk.

### Your QualysGuard 14-day free trial includes:

- A fully functional evaluation for up to three users
- Thousand of vulnerability checks, verified fixes and reports
- Free technical workshops, online training and technical support
- No financial obligation

To get your FREE trial, please complete this form:

Note: \* = Required



It is also known as Security Administrator's Integrated Network Tool

It detects the network vulnerabilities on any remote target in a non-intrusive manner

It gathers information regarding what type of OS is running and which ports are open

### 4 Steps to a SAINT™ Scan



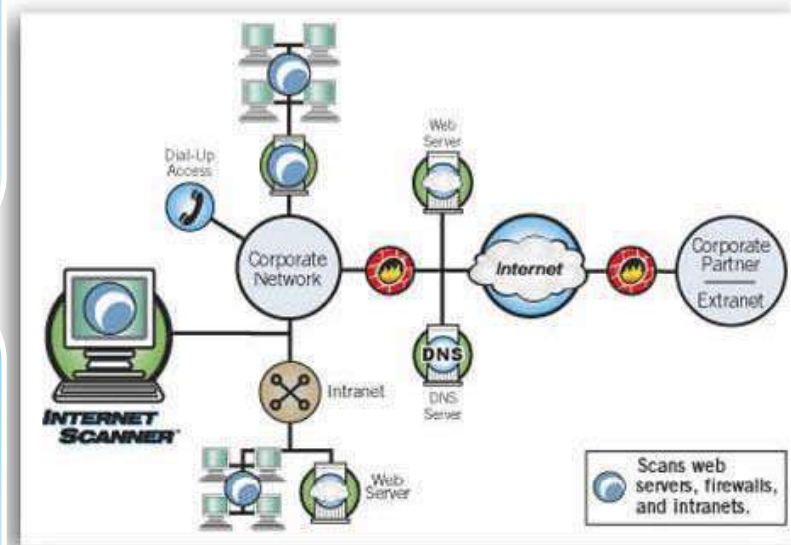


# ISS Security Scanner



Internet Security Scanner provides automated vulnerability detection and analysis of networked systems

It performs automated, distributed, or event-driven probes of geographically dispersed network services, OS, routers/ switches, firewalls, and applications and then displays the scan results



# ISS Security Scanner: Screenshot

The screenshot displays the ISS Internet Scanner interface. The main window is titled "ISS Internet Scanner - [Session4.session]". The interface is divided into several sections:

- Left Panel:** A tree view under "Vulnerabilities" listing various security issues, such as "accountuserpw test [1]", "Backup Privilege [1]", "getadmin [1]", "Modified Teardrop Attack [1]", "Restore Privilege [1]", "securitylog [1]", "Windows Key Permissions [1]", "Windows NT SMB logon DoS [1]", "All Access NetBIOS share - [1]", "Chargen Patch [1]", "DNS Predictable Query [1]", "echo [1]", "NetBIOS shares - null session [1]", "Network Monitor [1]", "oob\_crash [1]", "pwlen [1]", "regfile [1]", "regfile - permissions [1]", and "repair insecure [1]".
- Center Panel:** A table listing the details of the selected vulnerabilities. The table has columns for "Vulnerability Name", "Risk", and "Description".
- Right Panel:** A vertical toolbar with icons for "Start", "Unb...", and "IS...".
- Bottom Panel:** A status bar with tabs for "Properties", "Status", "Vulnerabilities", "Services", and "Users". Below the tabs is a text area showing system messages like "Identd server bound", "Sendmail pipe bug response server bound", "Sendmail identd bug response server bound", "Rsh spoof response server bound", "Rlogin spoof response server bound", and "Response server thread started".
- Footer:** A status bar at the bottom of the application window showing "For Help, press F1", "harmful", "1 Host(s)", and the time "10:46".

Vulnerability Name	Risk	Description
NetBIOS share C\$	Low	NetBIOS shares disks to world
NetBIOS share D\$	Low	NetBIOS shares disks to world
NetBIOS share print\$	Low	NetBIOS shares disks to world
repair insecure	Medium	Repair Directory Readable
DNS Predictable Query	Medium	DNS Predictable Query
getadmin	High	Getadmin Patch not applied
oob_crash	Medium	Vulnerable to out of band DOS attack on port 139
ssping	Medium	Ssping Patch not Applied
land	Low	Land denial of service attack.
PPT_patch	Low	Missing PowerPoint Security Patch
LM security	Low	Lan Manager Security
Chargen Patch	Medium	Chargen Patch not Applied
WINS Patch	Medium	WINS Patch not Applied
Modified Teardrop Attack	High	Modified teardrop attack blue screens Windows sys.
Windows NT SMB logon DoS	High	Windows NT denial of service attack
systemlog	Low	Windows NT System Log Accessible
securitylog	High	Windows NT Security Log Accessible
applog	Low	Readable NT Application Log
alerter	Low	Alerter and messenger services

Nessus is a vulnerability scanner which looks for bugs in software

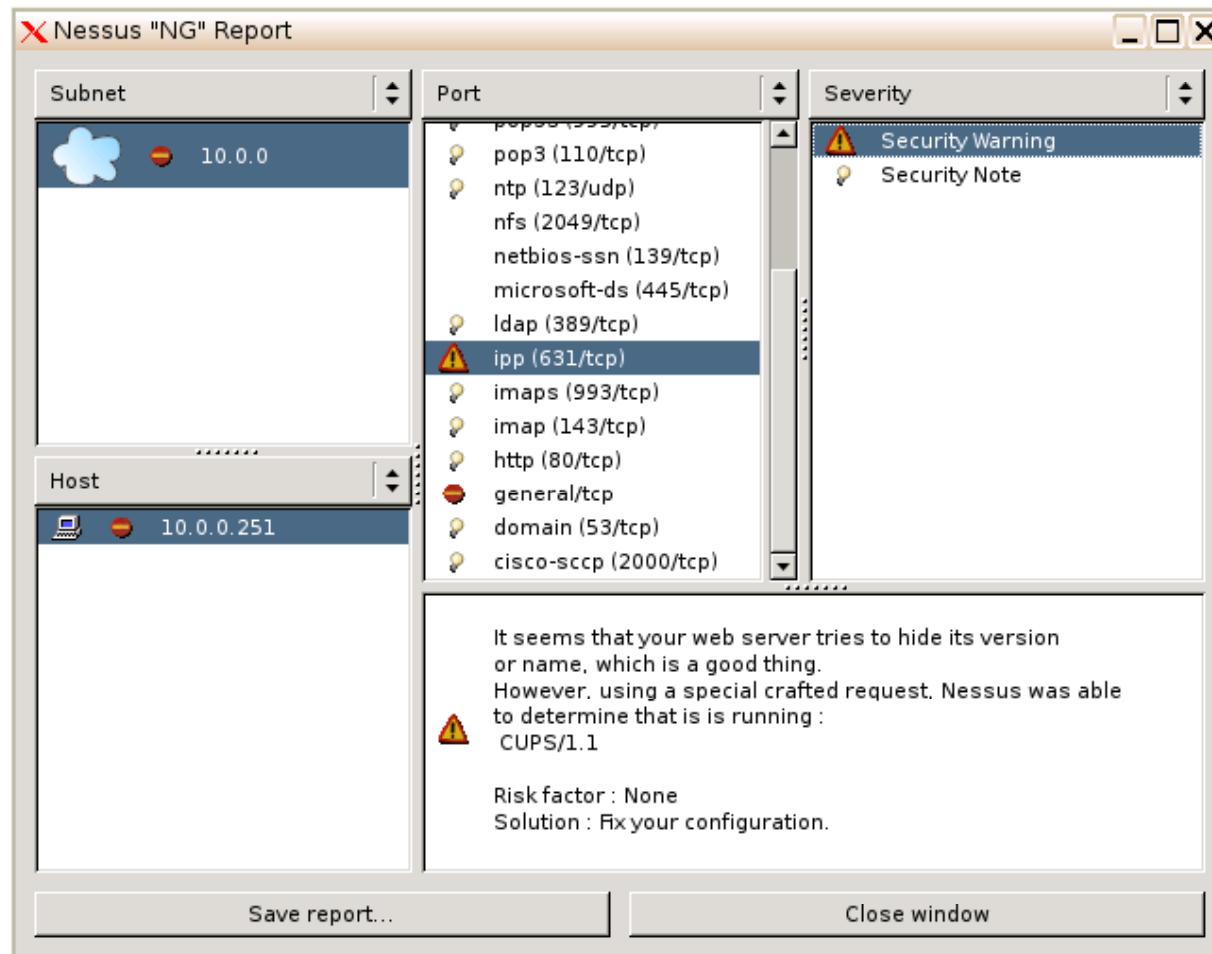
An attacker can use this tool to violate the security aspects of a software product

### Features:

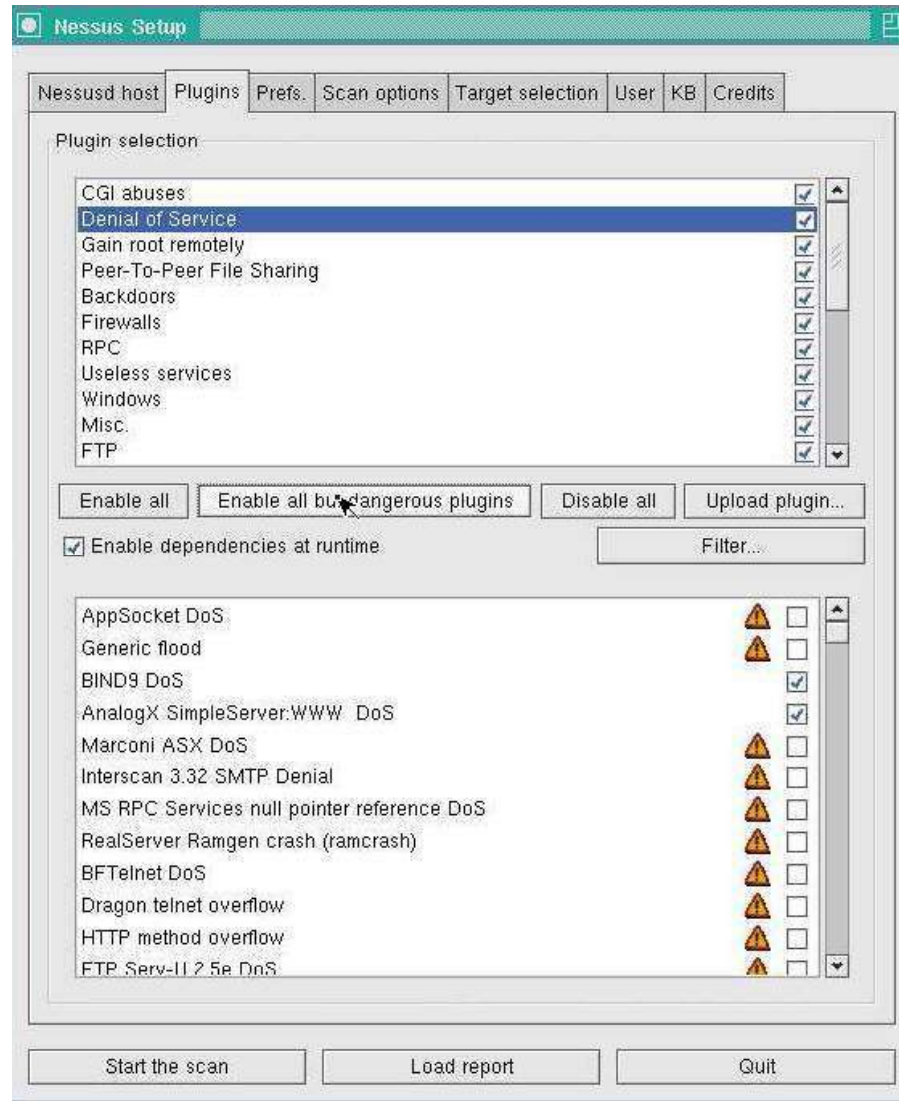
- Plug-in-architecture
- NASL (Nessus Attack Scripting Language)
- Can test unlimited number of hosts simultaneously
- Smart service recognition
- Client-server architecture
- Smart plug-ins
- Up-to-date security vulnerability database



# Nessus: Screenshot 1



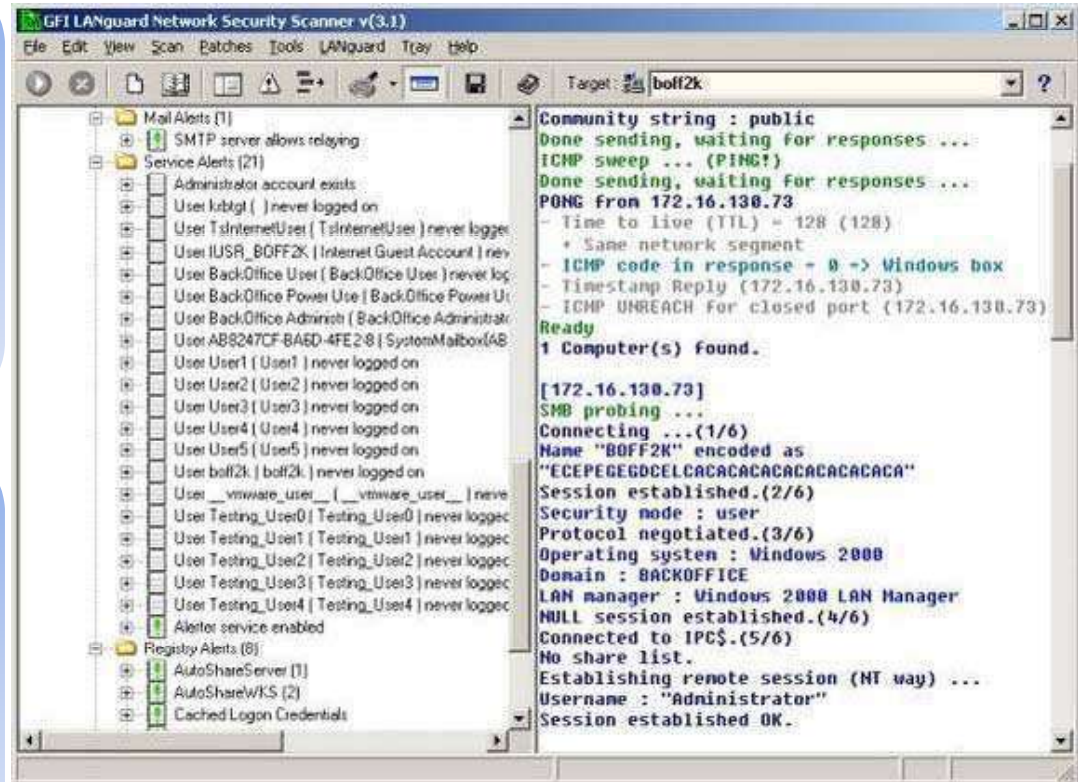
# Nessus: Screenshot 2





GFI LANGUARD analyzes the operating system and the applications running on a network and finds out the security holes present

It scans the entire network, IP by IP, and provides information such as the service pack level of the machine and missing security patches, to name a few



# GFI LANGuard Features

Fast TCP and UDP port scanning and identification

Finds all the shares on the target network

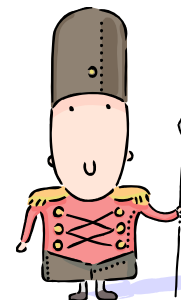
It alerts the pinpoint security issues

Automatically detects new security holes

Checks password policy

Finds out all the services that are running on the target network

Vulnerabilities database includes UNIX/ CGI issues





# SATAN (Security Administrator's Tool for Analyzing Networks)

Security-auditing tool developed by Dan Farmer and Weitse Venema

Examines UNIX-based systems and reports the vulnerabilities

Provides information about the software, hardware, and network topologies

User-friendly program with an X Window interface

Written using C and Perl languages. Thus to run SATAN, the attacker needs Perl 5 and a C compiler installed on the system

In addition, the attacker needs a UNIX-based operating system and at least 20MB of disk space





Retina network security scanner is a network vulnerability assessment scanner

It can scan every machine on the target network, including a variety of operating system platforms, networking devices, databases, and third party or custom applications

It has the most comprehensive and up-to-date vulnerability database and scanning technology



# Retina: Screenshot

The screenshot shows the Retina scanner interface with the following components:

- Address Bar:** 192.168.0.44
- Scanner - Default:** IP Range
- Find:** 192.168.0.0/24
- General:**
  - Address: 192.168.0.0/24
  - Report Date: 06/12/03 03:04:32 PM
  - Domain Name: neo.office.upstream.se
  - Ping Response: Host Responded
  - Avg Ping Response: 10 ms
  - Time To Live: 128
  - Traceroute: 192.168.0.44
- Audits:** 192.168.0.0/24
- NetBIOS:** Null Session
- Remote Access:** PCAnywhere
- IP Services:** TCP/IP Security
- Registry:** Auto Sharing Drive Problem - NT Server
- Registry:** Auto Sharing Drive Problem - NT Wks
- Registry:** MS RAS Logging
- Registry:** MSCHAPv2 VPN
- Registry:** NTFS 8 Dot 3
- Registry:** Printer Driver Sec
- Registry:** Shutdown without Logon
- Remote Access:** DCOM Enabled
- Remote Access:** Dialup Save Password
- Remote Access:** MS RAS Escort

**IP Services: TCP/IP Security**

**Description:** TCP/IP Security is not enabled. It is recommended for maximum security that you set up strict settings as to what ports you will allow incoming data to go to. For example, if your server only acts as a web server you should set the TCP/IP security options to be:  
 TCP Permit Only: 80,443  
 UDP Permit Only: none  
 IP Permit All

**Risk Level:** Medium

**How To Fix:** To configure TCP/IP security settings:  
 1. Open Control Panel

**Did you know...** You can easily enter a range of IP Addresses to scan from the Scanner Interface by typing CTRL + R.

Support  
 Links

Scan complete

Nagios is a host and service monitor designed to inform you of network problems before your clients, end-users, or managers do

### Features:

- Monitoring of network services (SMTP, POP3, HTTP, NNTP, PING, etc.)
- Monitoring of host resources (processor load, disk and memory usage, running processes, log files, etc.)
- Simple plugin design that allows users to easily develop their own host and service checks
- Ability to define network host hierarchy, allowing detection of and distinction between hosts that are down and those that are unreachable
- Contact notifications when service or host problems occur and get resolved (via email, pager, or other user-defined method)

# Nagios: Screenshot 1

The screenshot displays the Nagios web interface in a Netscape browser window. The interface is divided into several sections:

- Left Sidebar:** Contains navigation menus for 'General', 'Monitoring', and 'Configuration'. The 'Monitoring' menu is expanded, showing options like 'Home', 'Documentation', 'Tactical Overview', 'Status Detail', 'Status Overview', 'Status Summary', 'Status Grid', 'Status Map', '3-D Status Map', 'Service Problems', 'Network Outages', 'Trends', 'Availability', 'Alert History', 'Notifications', 'Log File', 'Comments', 'Downtime', 'Process Info', and 'Performance Info'.
- Current Network Status:** A box at the top left showing the last update time (Sun Jul 15 14:06:34 CDT 2007) and a message that the monitoring process is running.
- Host Status Totals:** A summary table showing 100 Up, 2 Down, 0 Unreachable, and 0 Pending hosts. A button for 'All Problems' shows 7.
- Service Status Totals:** A summary table showing 100 OK, 2 Warning, 0 Unknown, 14 Critical, and 10 Pending services. A button for 'All Problems' shows 46.
- Service Overview For All Host Groups:** A central section with six sub-tables:
  - Winbox Workstations (10 winbox-workst01):** Shows one host 'winbox01' with 'UP' status and '1 OK' service.
  - Redhat Servers (10 rhel01-server01):** Shows five hosts, all with 'UNREACHABLE' status.
  - Linux Servers (10 linux01-server01):** Shows five hosts, all with 'UP' status and '1 OK' service.
  - Mail Servers (10 mail01-server01):** Shows one host 'mail01' with 'UP' status and '1 OK' service.
  - Novell Servers (10 novell01-server01):** Shows two hosts, both with 'UP' status and '1 OK' service.
  - NT Domain Servers (10 nt-domain01-server01):** Shows two hosts, both with 'UP' status and '1 OK' service.

# Nagios: Screenshot 2

The screenshot shows the Nagios web interface in a Netscape browser window. The interface includes a navigation menu on the left, summary statistics at the top, and a detailed table of service statuses.

**Current Network Status**  
 Last Updated: Sun Jul 15 14:02:12 CDT 2001  
 Updated every 75 seconds  
 Nagios™ [www.nagios.org](#)  
 Logged in as [poller](#)  
 Monitoring process is running  
 \*No Plugins cannot be read out!  
 \*Service checks are being executed

**Host Status Totals**

Up	Down	Unreachable	Pending
26	0	0	0

**Service Status Totals**

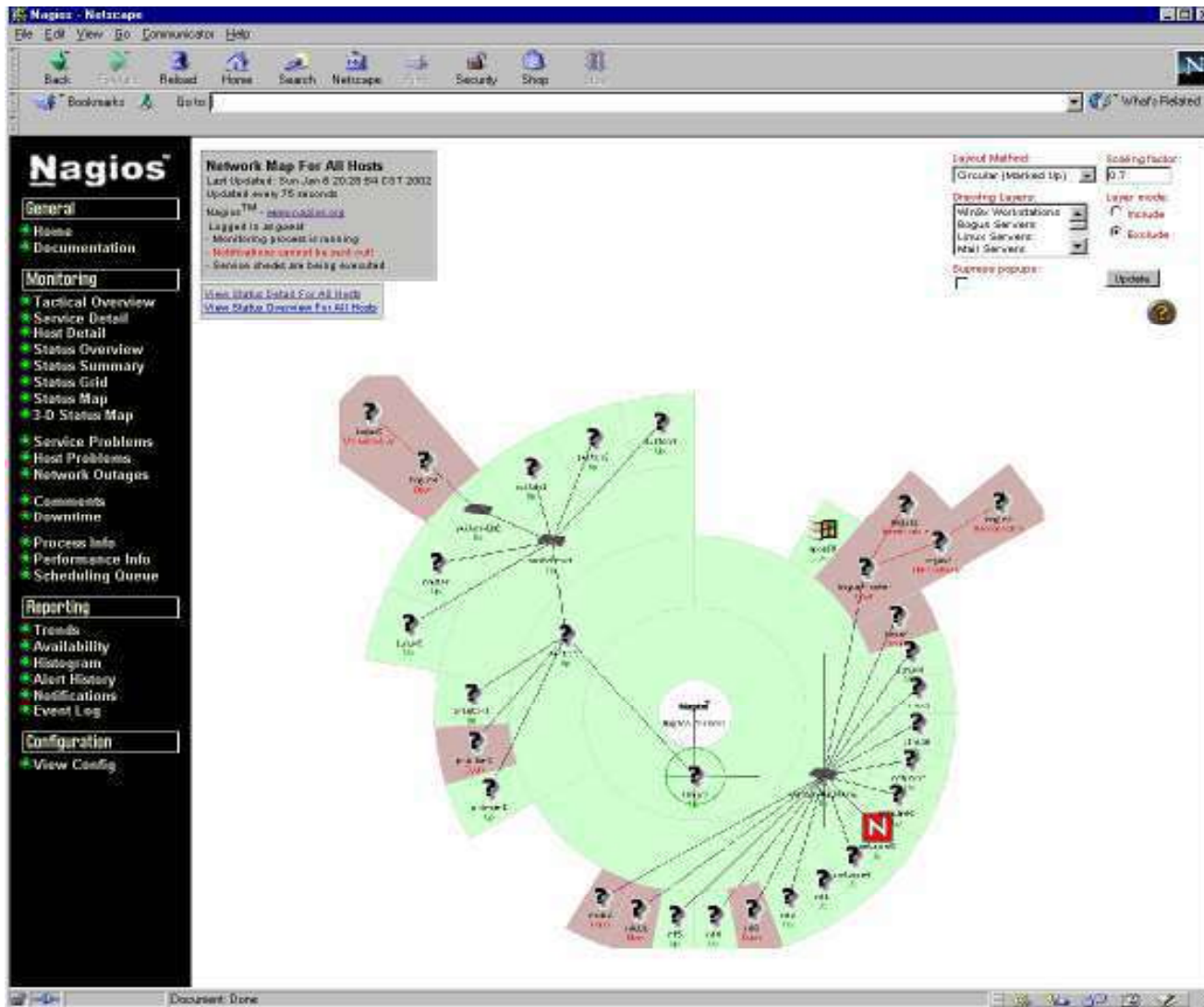
OK	Warning	Unknown	Critical	Pending
102	2	0	14	10

**Service Details For All Hosts**

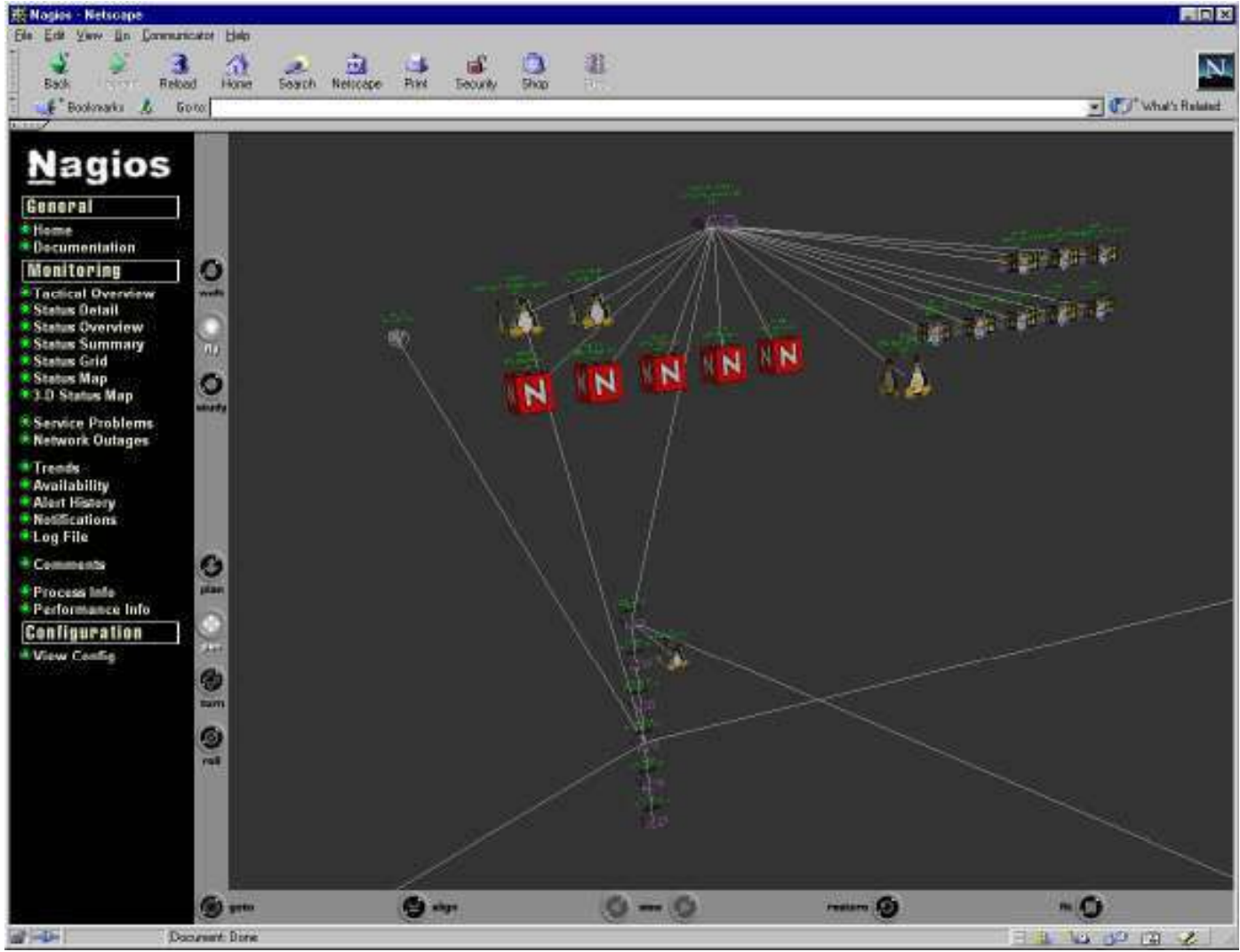
Host	Service	Status	Last Check	Duration	Attempt	Service Information
xxxxxx00	PING	CRITICAL	07-15-2001 13:59:39	4d35:40m:17s	10	CRITICAL - Plugin timed out after 30 seconds
xxxx01	SSH	CRITICAL	07-15-2001 14:00:35	4d35:50m:40s	10	(Service Check Timed Out)
xxxx01	SSH	CRITICAL	07-15-2001 14:00:35	4d35:50m:40s	10	CRITICAL - Plugin timed out after 30 seconds
xxxx02	PING	CRITICAL	07-15-2001 13:59:09	4d35:44m:27s	10	CRITICAL - Plugin timed out after 30 seconds
xxxx02	SSH	CRITICAL	07-15-2001 13:59:39	4d35:40m:26s	10	(Service Check Timed Out)
xxxx02	SSH	CRITICAL	07-15-2001 14:00:35	4d35:42m:7s	10	CRITICAL - Plugin timed out after 30 seconds
xxxx02	SSH	CRITICAL	07-15-2001 13:57:39	4d35:30m:26s	10	(Service Check Timed Out)
xxxx04	PING	CRITICAL	07-15-2001 13:59:09	4d35:40m:26s	10	CRITICAL - Plugin timed out after 30 seconds
xxxx04	SSH	CRITICAL	07-15-2001 13:59:39	4d35:40m:26s	10	(Service Check Timed Out)
xxxx05	PING	CRITICAL	07-15-2001 14:00:40	4d35:41m:7s	10	CRITICAL - Plugin timed out after 30 seconds
xxxx05	SSH	CRITICAL	07-15-2001 13:57:39	4d35:30m:26s	10	(Service Check Timed Out)
xxxx06	Total Cache Ratio	WARNING	07-15-2001 12:59:45	4d35:20m:24s	30	Total cache buffer = 21463
xxxx06	Total Cache Ratio	WARNING	07-15-2001 14:01:01	4d35:27m:14s	30	Total cache buffer = 22991
xxx0	Ethical Hacker Use	CRITICAL	07-15-2001 14:02:28	3d 15:21m:44s	30	Physical memory problems - 506.4 MB (99%) at 511.4 MB used
xxxx07	SSH	CRITICAL	07-15-2001 14:02:40	1d 15:36m:15s	10	CRITICAL - Plugin timed out after 30 seconds
xxxx07	SSH	CRITICAL	07-15-2001 14:01:20	1d 15:26m:54s	10	Timeout: No response from 134.04.02.77



# Nagios: Screenshot 3



# Nagios: Screenshot 4



# PacketTrap's pt360 Tool Suite

It consolidates the PacketTrap free network management tools into a real time reporting solution and replaces disparate IT tools from multiple vendors

It also includes integration with browser-based open source networking tools such as Nagios, OpenNMS, and others

## Features:

Real Time Reporting

Dashboard

Favorites

Recent Tools Lists

Networks

Custom Tools and Categories





# PacketTrap's pt360 Tool Suite: Screenshot

The screenshot displays the PT360 ToolSuite application window. At the top, there is a menu bar (File, Edit, Favorites, Tools, Window, Help) and a toolbar with icons for various tools: Ping Scan, Enhanced Ping, Graphical Ping, DNS Audit, WHOIS, Port Scan, MAC Scan, SNMP Scan, WMI Scan, Wake on LAN, Trace Route, Traffic Jam, and TFTP Server. Below the toolbar is the 'PacketTrap ptControl Network Dashboard' section, which includes a 'Critical Systems' tab and several monitoring panels:

- www.PacketTrap.com (www.PacketTrap.com) Availability Chart:** A line graph showing response times in milliseconds over time. The y-axis ranges from 0 to 640 ms, and the x-axis shows time from 3:38 PM to 11:45 AM. The chart shows several peaks, with the highest reaching approximately 633 ms. Summary: (3) (0) (Avg 112ms, Max 633ms, Last 62ms, 11:45 AM)
- Critical Servers Availability List:** A table listing servers and their response times:
 

buildmachine.jetstreamnetworks.local	0 ms
projectserver.jetstreamnetworks.local	0 ms
mediawiki.jetstreamnetworks.local	482 ms
dc-packettrap.jetstreamnetworks.local	0 ms
bugzilla.jetstreamnetworks.local	0 ms
wiki.jetstreamnetworks.local	0 ms
dc-file.jetstreamnetworks.local	0 ms
exchange-packettrap.jetstreamnetworks.local	0 ms
autodiscover.jetstreamnetworks.com	0 ms
- PacketTrap Website (www.PacketTrap.com) Availability Gauge:** Two gauges showing 'Current Response 62 ms' and 'Avg Packet Loss 0 %'.
- PacketTrap Blog Server Availability Text:** Shows the URL 'blog.packettrap.com' and summary: (2) (0) (Avg 62ms, Max 62ms, Last 62ms, 11:45 AM)

At the bottom of the dashboard, there are buttons for 'Quick Launch' and 'Dashboard'.

NIKTO is an open source web server scanner

It performs comprehensive tests against webservers for multiple items

It tests web servers in the shortest time possible

Uses RFP's libwhisker as a base for all network functionality

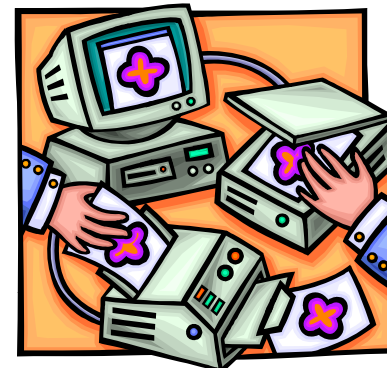
For easy updates, the main scan database is of CSV format

SSL support

Output to file in simple text, html, or CSV format

Plug-in support

Generic and server type specific checks



# SAFEsuite Internet Scanner, IdentTCPScan

## SAFEsuite Internet Scanner

- Developed by Internet Security Systems (ISS) to examine the vulnerabilities in Windows NT networks
- Requirements are Windows NT and product license key
- Reports all possible security gaps on the target system
- Suggests possible corrective actions
- Uses three scanners: Intranet, Firewall, and Web Scanner



## IdentTCPScan

- Examines open ports on the target host and reports the services running on those ports
- It is a special feature that reports the UIDs of the services





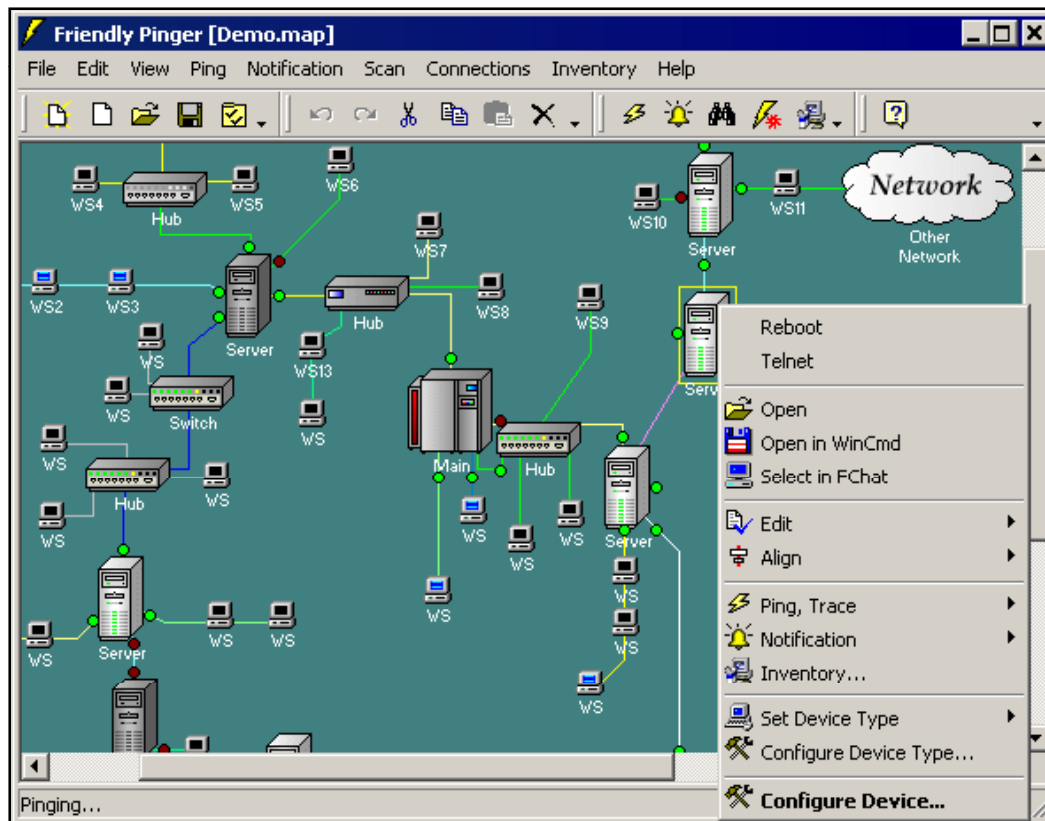
## Draw Network Diagrams of Vulnerable Hosts

# CEH<sup>TM</sup> FriendlyPinger

Certified Ethical Hacker

A powerful and user-friendly application for network administration and monitoring

It can be used for pinging of all devices in parallel at once and in assignment of external commands (like telnet, tracer, net.exe) to devices



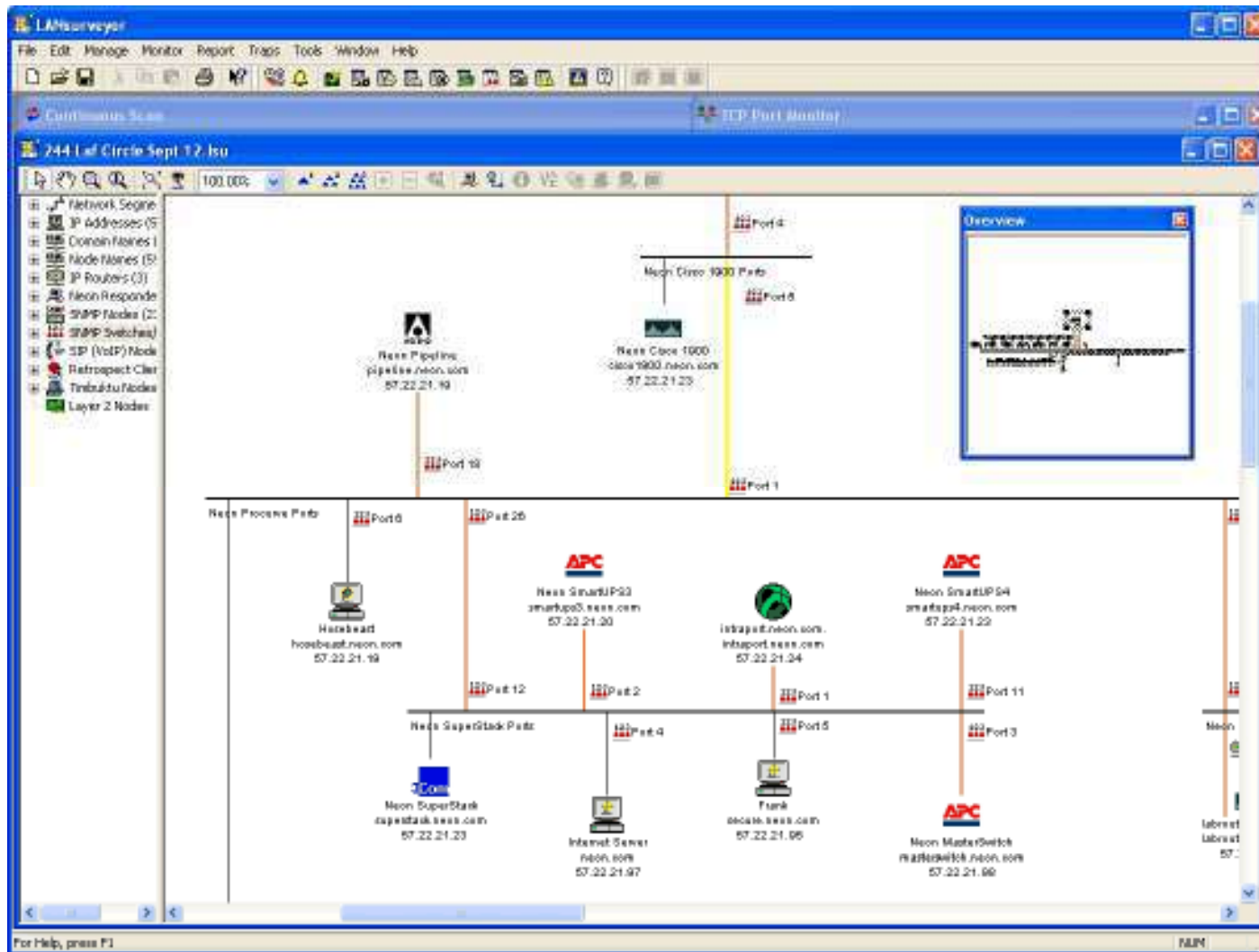
VisioLANsurveyor automatically discovers your network and produces comprehensive and easy-to-view network maps that can be exported into Microsoft Office

## Features:

- Automatically discovers and diagrams network topology
- Generates network maps in Microsoft Office® Visio®
- Automatically detects new devices and changes made to the network topology
- Performs inventory management for hardware and software assets
- Directly addresses PCI compliance and other regulatory requirements

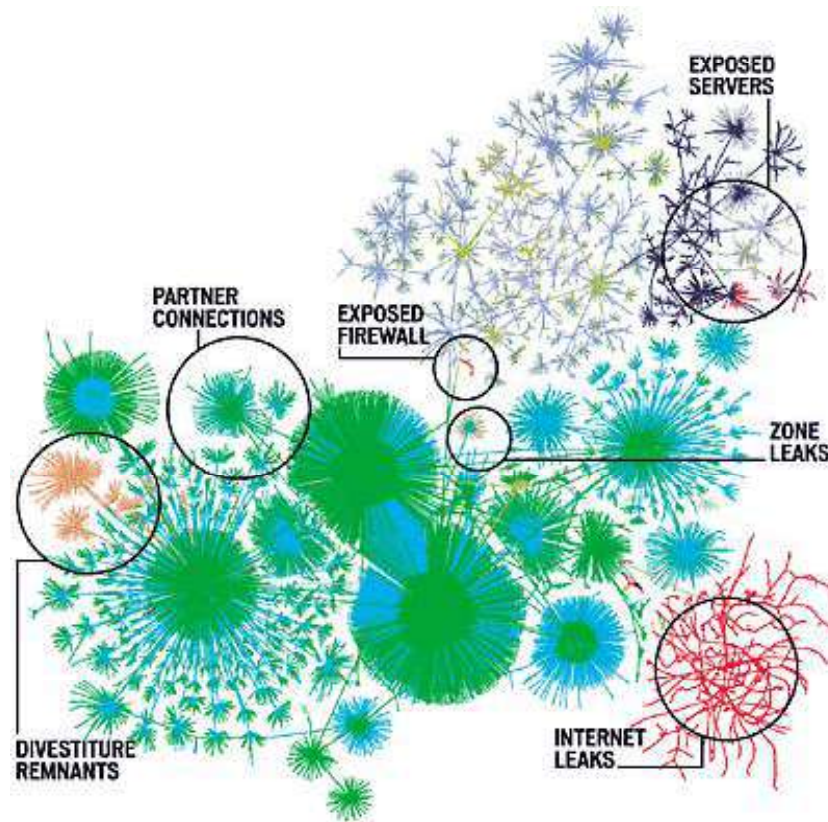


# LANsurveyor: Screenshot





Lumeta's IPsonar actively scans the network to collect all data related to these factors via Network Discovery, Host Discovery, Leak Discovery, and Device Fingerprint Discovery



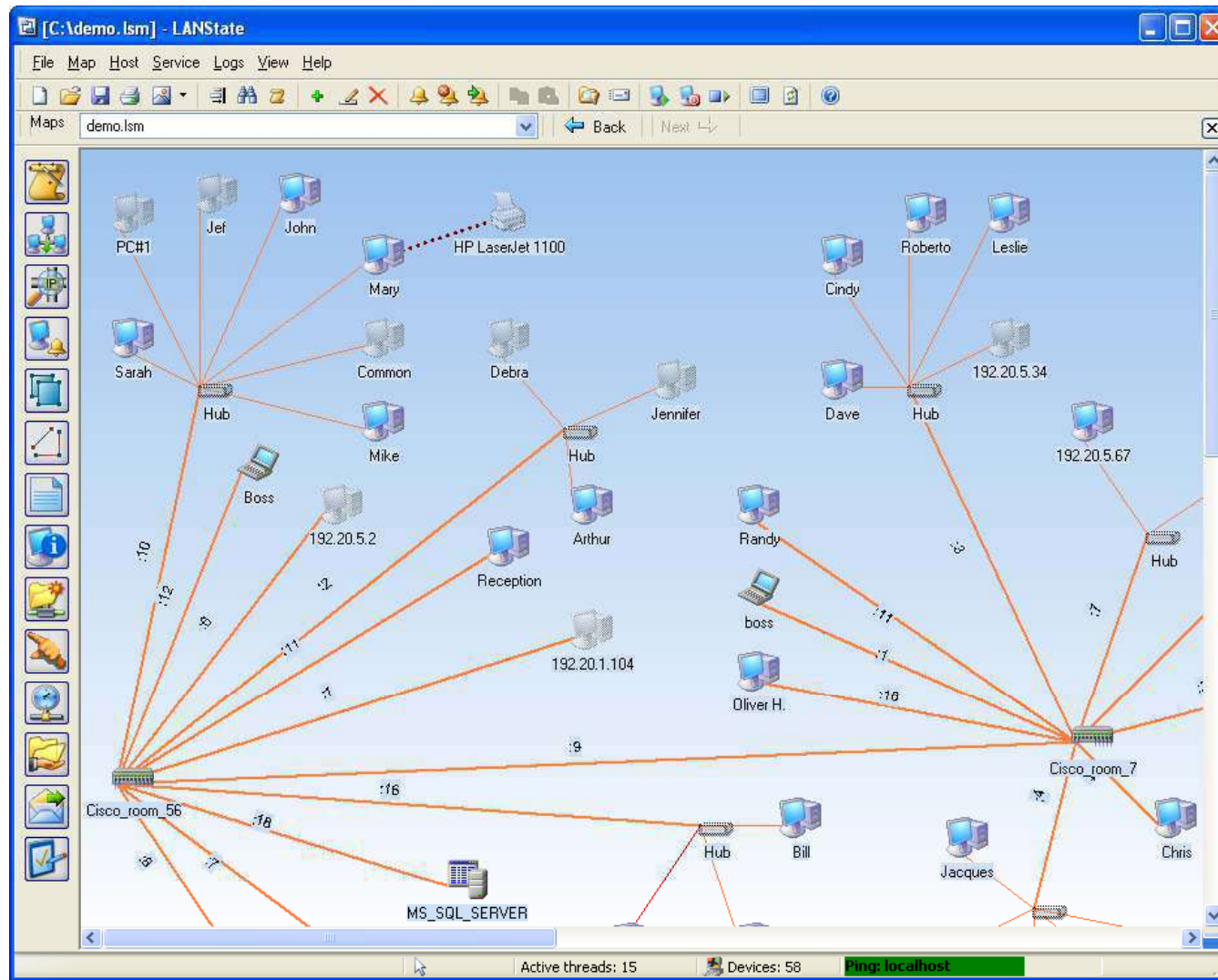
LANState is a network mapping, monitoring, management, and administration software solution for corporate Microsoft Windows networks

## Benefits:

- LANState builds a network map automatically by scanning Windows network neighborhood or IP-address range
- Save your network map for future use, print it, and export it to a bitmap file
- Be notified by background device monitoring via a screen message, sound, or e-mail when your servers go down or start working



# LANState: Screenshot



Insightix Visibility obtains a complete inventory of all network devices, including firewalled, unmanaged and virtual devices, and provides location information and a full list of associated properties

## Features:

- Complete IT Asset Discovery – It delivers a comprehensive inventory of every device on the network, including firewalled, unmanaged and virtual devices, and provides location information and a full list of associated properties
- Accurate Network Topology Map – It maps the entire physical network topology, including all devices, such as workstations, servers, printers, wireless access points, VoIP phones, switches, routers, and more
- Real-Time Change Detection – It continuously monitors the network for any changes made to the network and/or any of the devices on the network

IPCheck Server Monitor helps organizations to monitor critical network resources and detect system failures or performance problems immediately, thus minimizing downtimes and their economic impact

## Features:

- Powered by Paessler's reliable IPCheck<sup>TM</sup> technology
- Remote Management via web browser, PocketPC, or Windows client
- Notifies users about outages by email, ICQ, or pager/SMS, and more
- Monitors network services with its comprehensive sensor type selection
- Multiple location monitoring using secure Remote Probes



# IPCheck Server Monitor: Screenshot 1

**IPCheck Server Monitor** PAESSLER

Home My Account Administration Add New Group Help Logout logged in as beta@paessler.com

**Paessler GmbH (Paessler Support Team)** Refresh Edit >

**Main Server (Dallas, TX)** Edit >

**www.paessler.com** Edit >

● PING	PING	OK 145 ms		Edit >
● HTTP	http	OK 867 ms		Edit >
● FTP	ftp	OK 449 ms		Edit >
● HTTP ADV	Homepage Content Checks	OK 1455 ms		Edit >
● HTTP	PRTG Website	OK 1488 ms		Edit >

**updates.paessler.com** Edit >

● HTTP	http	OK 877 ms		Edit >
--------	------	-----------	--	--------

**www.bello-monitors-the.net** Edit >

● PING	PING Sensor2	OK 140 ms		Edit >
● HTTP	HTTP Sensor3	OK 1132 ms		Edit >

**Sensor Summary**

● 19 Sensor(s) up and running well

**Messages/Errors** More

08:19:28 rizzo.paessler.com PING6 (PING) UP - OK 87 ms  
 08:19:28 rizzo.paessler.com PING6 (PING) WARNING - Lost 30  
 06:43:41 www.bello-monitors-the.net HTTP Sensor3 (HTTP) UP -  
 06:43:08 www.bello-monitors-the.net HTTP Sensor3 (HTTP) WAF  
 06:51:34 rizzo.paessler.com PING6 (PING) UP - OK 88 ms  
 06:51:33 rizzo.paessler.com PING6 (PING) WARNING - Lost 30  
 06:47:50 www.bello-monitors-the.net PING Sensor2 (PING) UP -

**Activity** More

10:32:15 rizzo.paessler.com PING PING6: OK 89 ms  
 10:32:11 mailx.paessler.com SMTP Secondary MX: OK 31 ms  
 10:32:09 mail.paessler.com POP3 POP3 (External Mail Clients):  
 10:32:05 www.bello-monitors-the.net PING PING Sensor2: OK 1  
 10:32:05 www.bello-monitors-the.net PING PING Sensor3: OK 1  
 10:32:05 www.bello-monitors-the.net PING PING Sensor1: OK 1  
 10:32:05 www.bello-monitors-the.net HTTP PRTG Website: OK 1488 ms  
 10:32:05 www.bello-monitors-the.net PING PING: OK 145 ms  
 10:32:05 www.bello-monitors-the.net HTTP HTTP Sensor3: OK 1

**Server Menu**

- Edit
- Add Sensor
- Traceroute
- Pause/Resume
- Fold/Unfold
- Sort Sensors
- Duplicate Server
- Delete Server

# IPCheck Server Monitor: Screenshot 2

**IPCheck Server Monitor - "support@paessler.com" @ 10.0.0.193**

File My Account Add Help

Disconnect Refresh Now Web Home Add Group Add Server Add Sensor Help

Connected to account support@paessler.com @ 10.0.0.193

**Main Server (Dallas\_TX) (Up:8)**

www.paessler.com	PING	PING	Up	OK 144 ms
	HTTP	http	Up	OK 777 ms
	FTP	ftp	Up	OK 428 ms
	HTTP ADV	Homepage Content Checks	Up	OK 801 ms
updates.paessler.com	HTTP	PRTG Website	Up	OK 301 ms
	HTTP	http	Up	OK 301 ms
www.bello-monitors-the.net	PING	PING Sensor2	Up	OK 301 ms
	HTTP	HTTP Sensor3	Up	OK 301 ms

**DSL Connection HP7 (Up:9)**

First External Hop	PING	PING2	Up	OK 301 ms
DSL Router HP7 (Q5C)	PING	PING1	Up	OK 301 ms
mail.paessler.com	SMTP	Primary MX	Up	OK 301 ms
	PING	ping	Up	OK 3 ms

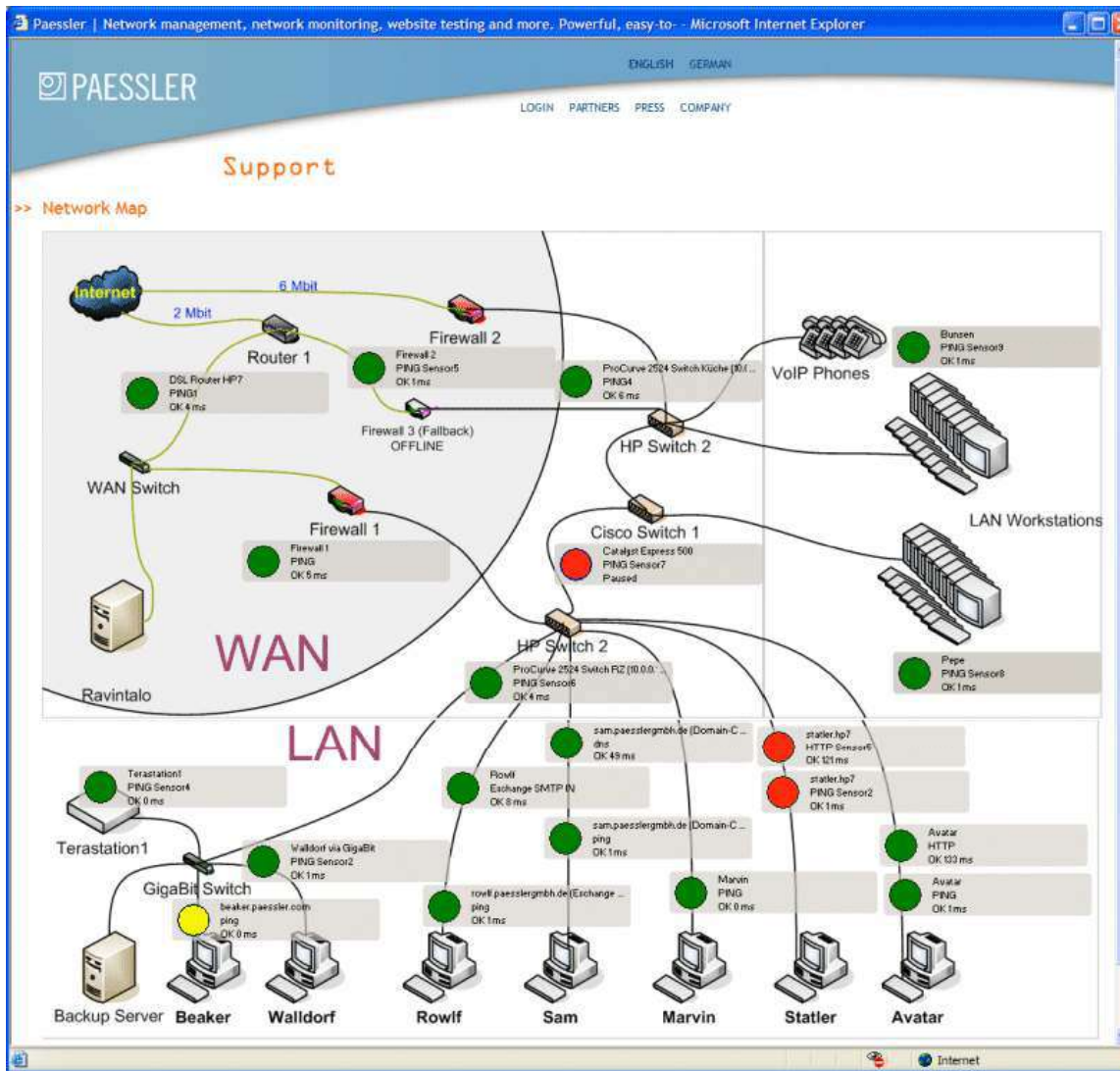
**Recent Messages**

- 15.06.2005 08:19:29: rizzo.paessler.com PING6 (PING) UP - OK 67 ms
- 15.06.2005 08:19:28: rizzo.paessler.com PING6 (PING) WARNING - Lost 30000 ms (Code: 11010)
- 15.06.2005 06:43:41: www.bello-monitors-the.net HTTP Sensor3 (HTTP) UP - OK 1131 ms
- 15.06.2005 06:43:08: www.bello-monitors-the.net HTTP Sensor3 (HTTP) WARNING - Slow 27410 ms
- 15.06.2005 05:51:34: rizzo.paessler.com PING6 (PING) UP - OK 66 ms

Up:19 Server Time: 15.06.2005 10:47:38 Version: 5.0.1.229 30s



# IPCheck Server Monitor: Screenshot 3



PRTG Traffic Grapher is an easy to use Windows software for monitoring and classifying the bandwidth's usage

It provides system administrators with live readings and long-term usage trends for their network devices

## Features:

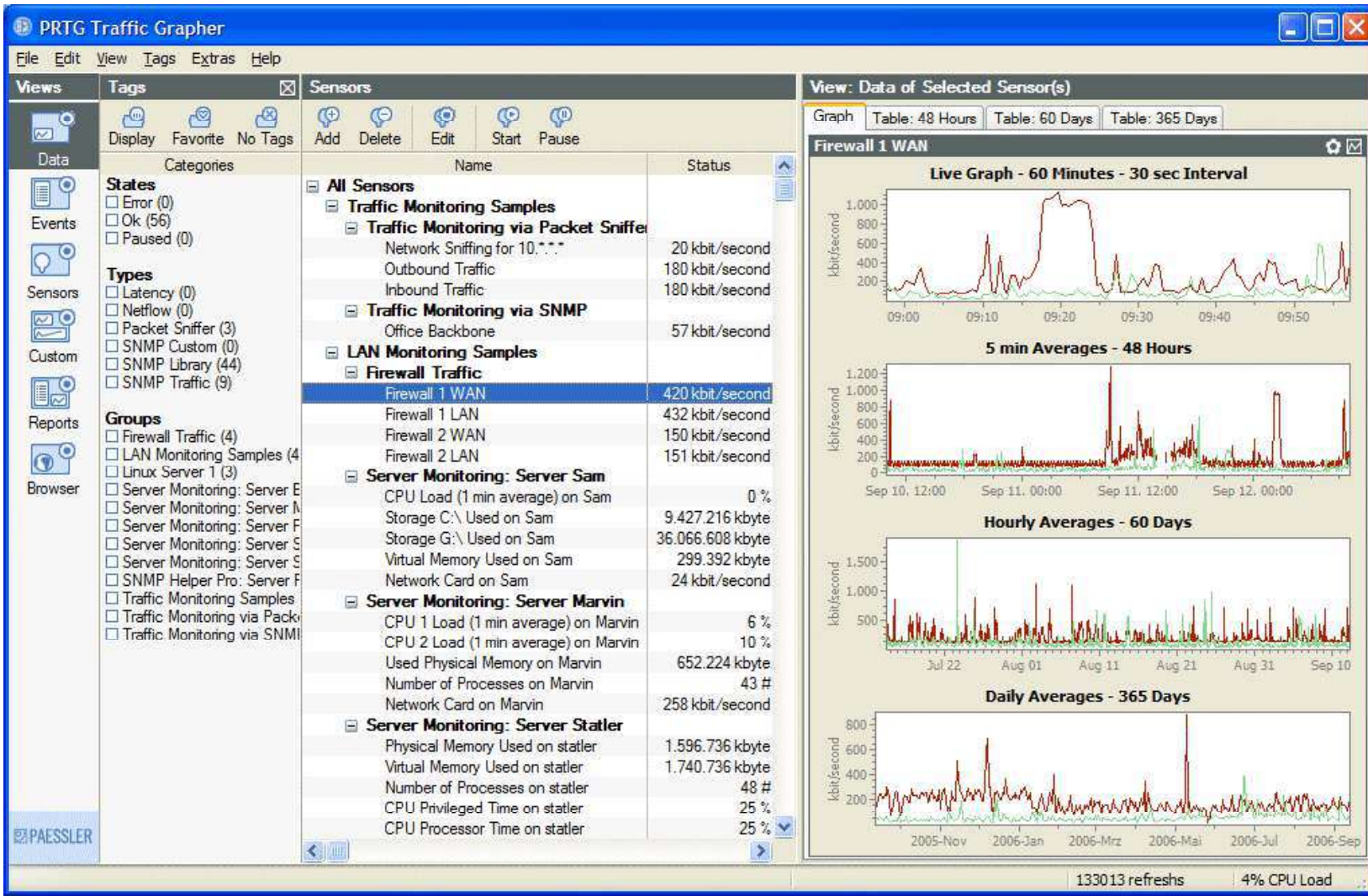
Avoid bandwidth and server performance bottlenecks

Find out what applications or what servers use up your bandwidth

Deliver better quality of service to your users by being proactive

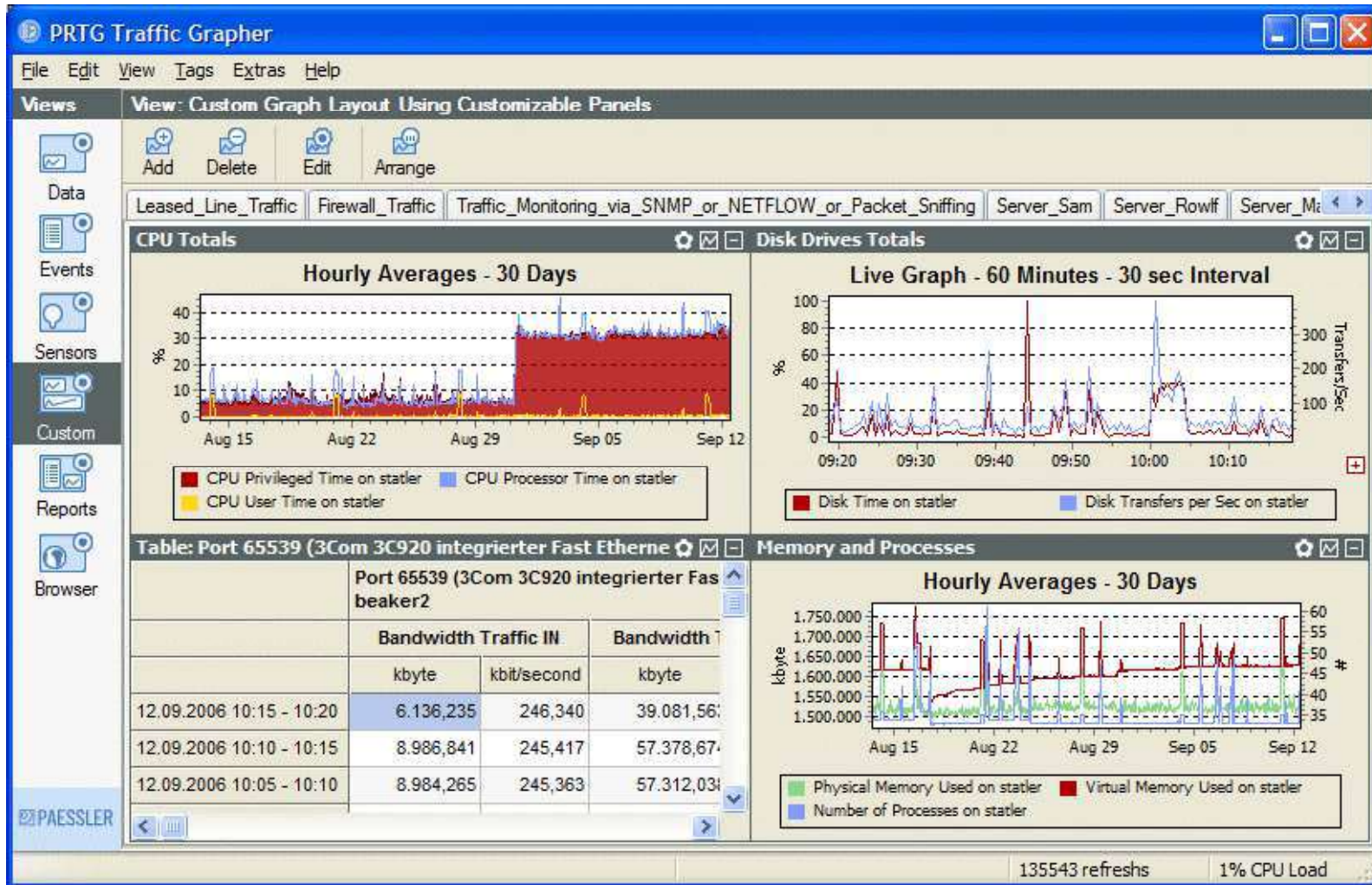
Reduce costs by buying bandwidth and hardware according to the actual load

# PRTG Traffic Grapher Screenshot: Network Traffic Monitoring





# PRTG Traffic Grapher Screenshot: Customizable Screen Layout



# PRTG Traffic Grapher Screenshot: Access Monitoring Data from Anywhere Using a Web Browser

View: Web Browser

Back Forward Home Refresh Stop

http://10.0.0.200/Server\_Statler/panel.htm?timeout=60&=4position=0

**PRTG Traffic Grapher** PAESSLER

Logged in as admin Logout Refresh: Off 15s 60s 5min

PRTG Demo Website > Custom Graphs > Server\_Statler

## Server\_Statler

**CPU Totals**  
 Hourly Averages - 30 Days

**Disk Drives Totals**  
 Live Graph - 60 Minutes - 30 sec Interval

**Memory and Processes**  
 Hourly Averages - 30 Days

Table: Port 65539 (3Com 3C920 integrierter Fast Ethernet-Controller (3C905C-TX kompatibel)) on beaker2 (48 Hours, 5 min Averages)

Port 65539 (3Com 3C920 integrierter F			
	Bandwidth kbyte	Traffic IN kbit/second	Bandwidth kbyte
12.09.2006 11:20 - 11:25	3.420,451	245,276	21.722,90
12.09.2006 11:15 - 11:20	9.027,117	246,525	57.439,54
12.09.2006 11:10 - 11:15	9.008,676	246,030	57.488,64
12.09.2006 11:05 - 11:10	10.658,862	291,077	57.515,86
12.09.2006 11:00 - 11:05	9.718,758	265,413	57.605,80

12.09.2006 11:22:21

Admin Contact  
 Homepage

PRTG Traffic Grapher V7.1.0.217 Netflow Edition LocalDev © 2003-2006 Paessler AG



# Preparing Proxies

# Proxy Servers

Proxy is a network computer that can serve as an intermediate for connection with other computers



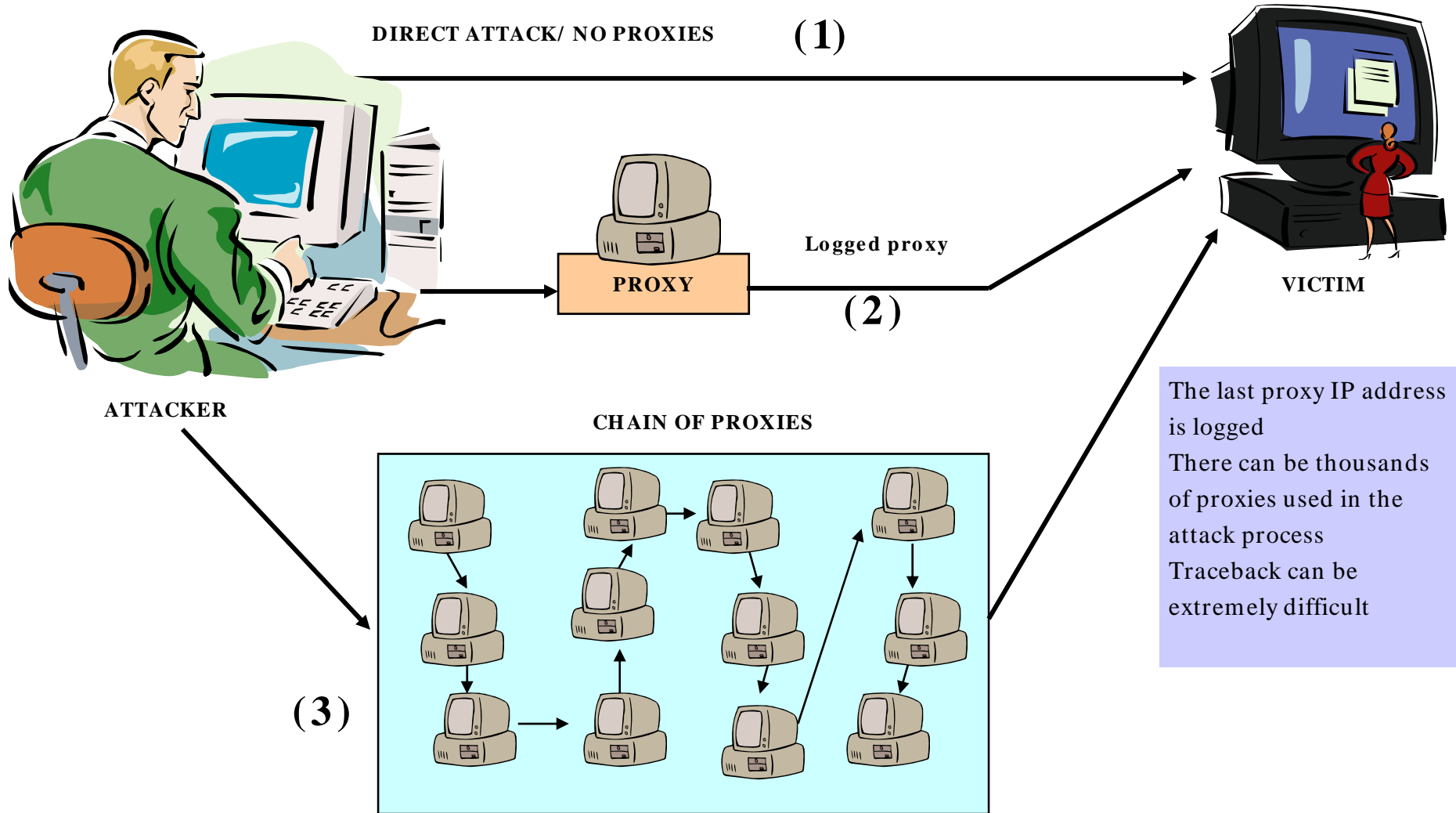
They are usually used for the following purposes:

- As a firewall, a proxy protects the local network from outside access
- As an IP addresses multiplexer, a proxy allows the connection of a number of computers to the Internet when having only one IP address
- Proxy servers can be used (to some extent) to anonymize web surfing
- Specialized proxy servers can filter out unwanted content, such as ads or 'unsuitable' material
- Proxy servers can afford some protection against hacking attacks





# Use of Proxies for Attack



The last proxy IP address is logged  
There can be thousands of proxies used in the attack process  
Traceback can be extremely difficult

# Free Proxy Servers

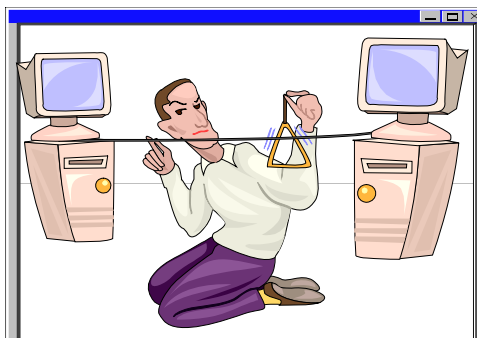
Attacks using thousands of proxy servers around the world are difficult to trace

Thousands of free proxy servers are available on the Internet

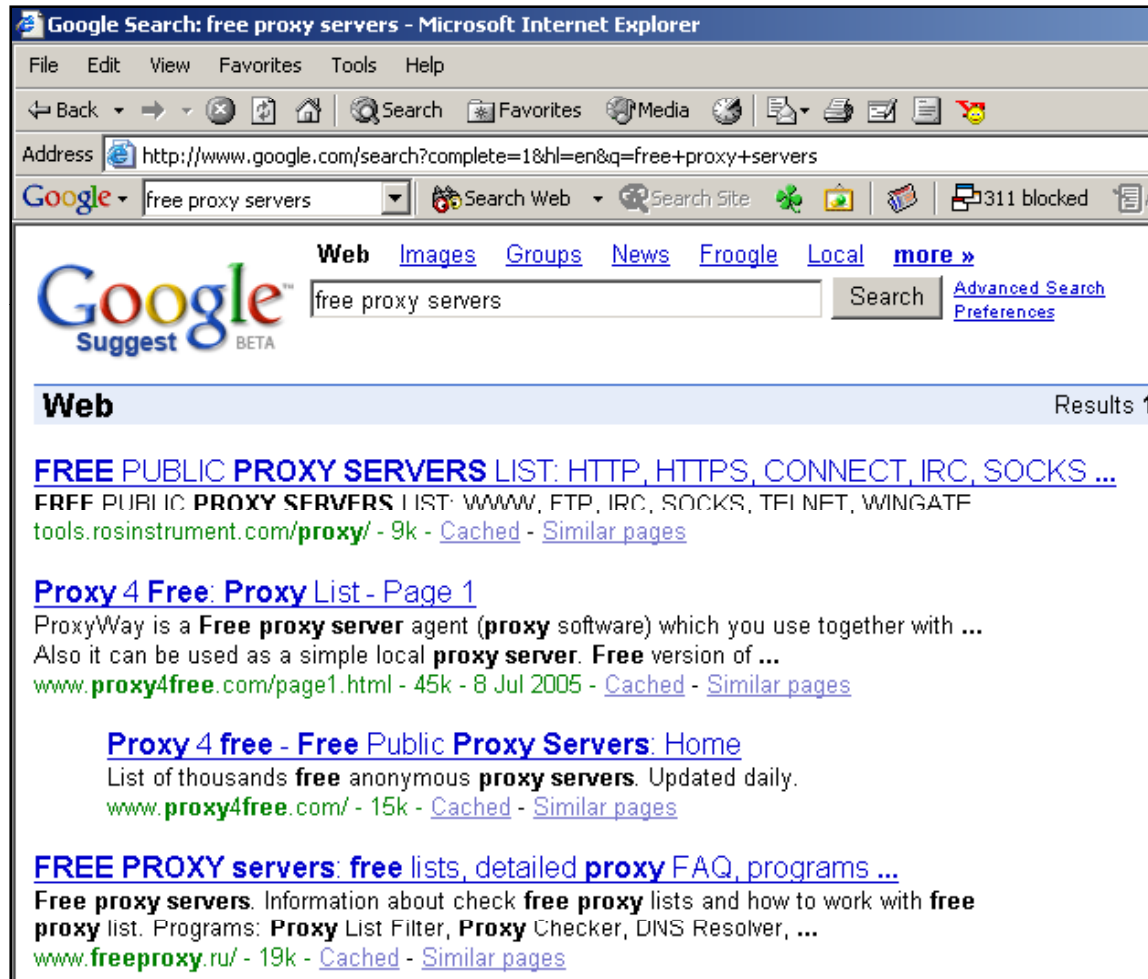
Search for “free proxy servers” in Google

Some of them might be a honeypot to catch hackers red-handed

Using proxy servers can mask your trace

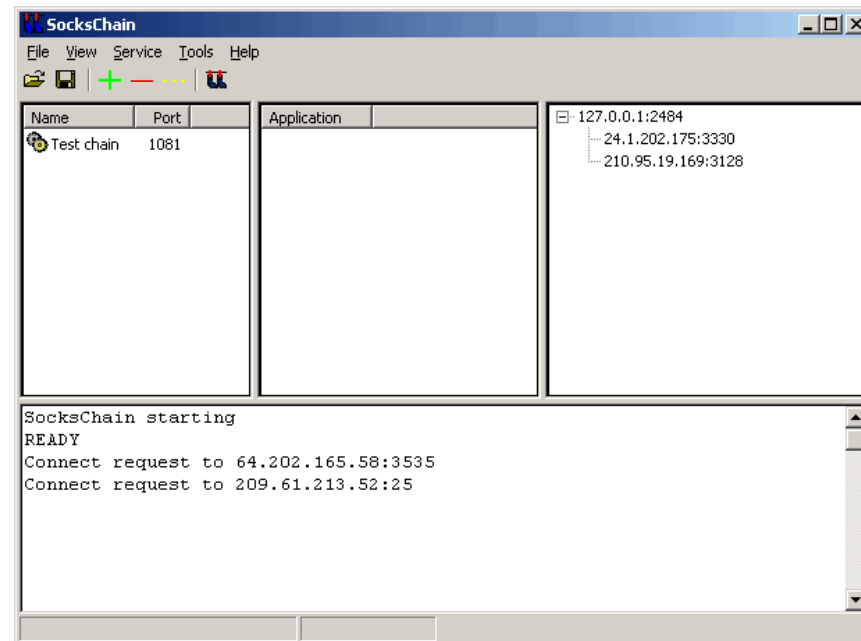


# Free Proxy Servers (cont'd)



SocksChain is a program that works through a chain of SOCKS or HTTP proxies to conceal the actual IP-address

SocksChain can function as a usual SOCKS-server that transmits queries through a chain of proxies



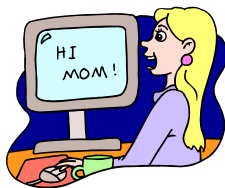
# Proxy Workbench

Proxy Workbench is a small proxy server which resides inside the network and monitor's connection

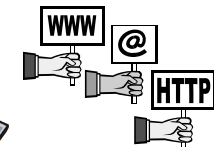
## Configuration:

Install Proxy Workbench

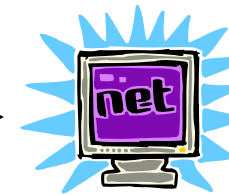
Configure the clients to use this proxy IP to connect to port 8080



User



Proxy Server



Internet

# Proxy Workbench: Screenshot

The screenshot displays the Proxy Workbench application window. The title bar reads "Proxy Workbench" and the menu bar includes "File", "View", "Tools", and "Help". The toolbar contains various icons for file operations and monitoring. The main interface is divided into several sections:

- Monitoring:** Shows "Monitoring: 192 (0.0.0.192)".
- Details for Dead (09:28:55.800):** This section shows a network diagram with a lightning bolt icon and text: "Remote connection request accepted 09:28:55.420". Below it, a yellow arrow icon is highlighted with a dashed red box, with text: "676 bytes of data has been".
- Real time data for Dead (09:28:55.800):** This section displays a list of HTTP headers and request details:

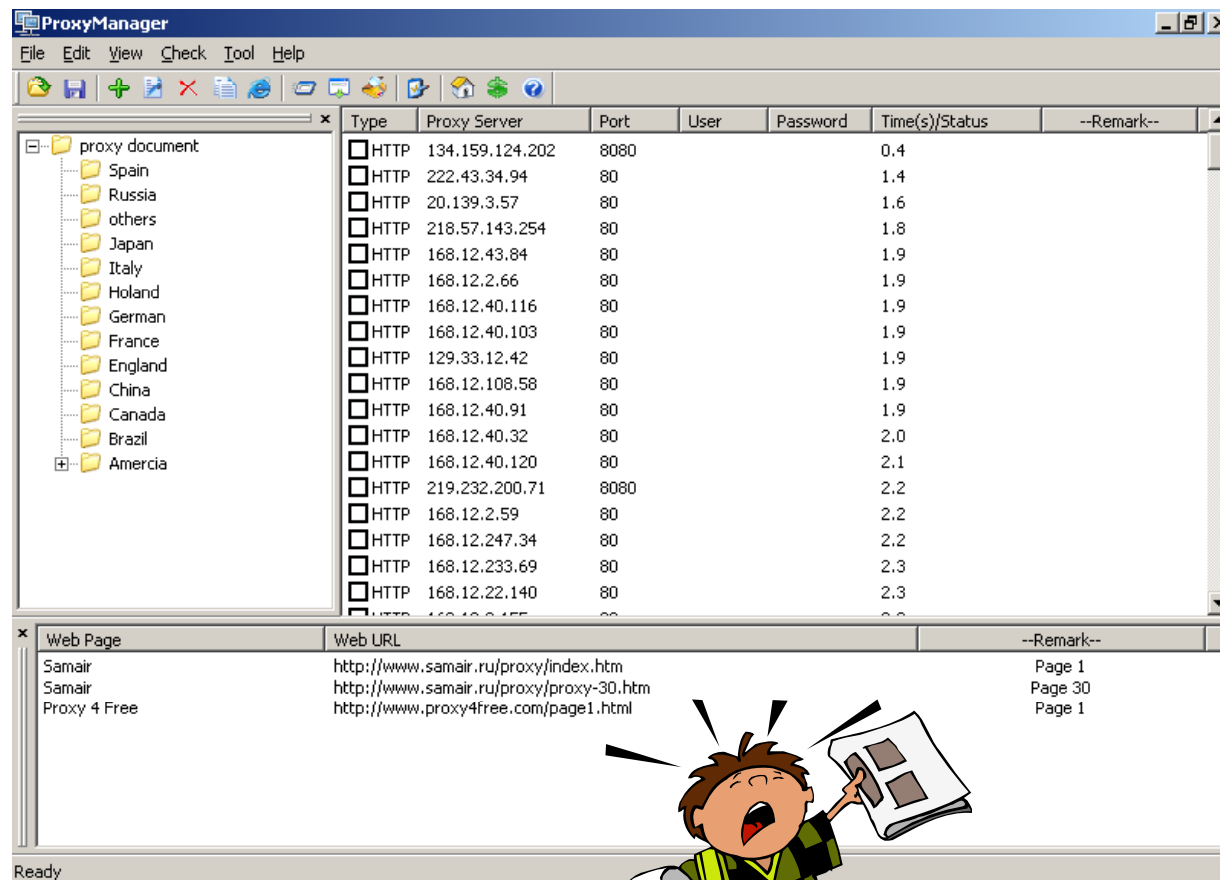
```
GET http://www.tcpiq.com/tcpiq/spellcheck/inc/SpellChe
Accept: */*
Referer: http://www.tcpiq.com
Accept-Language: en-au
Proxy-Connection: Keep-Alive
If-Modified-Since: Sun, 24 Jun 2001 05:55:34 GMT
If-None-Match: "d0b0e24872fcc01:29f963"
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Window
Host: www.tcpiq.com
Pragma: no-cache
```
- Left Panel:** A tree view under "All Activity" shows "HTTP (80)" with a list of "Dead" events, including "Dead With Error (09:28:47.790)" and several "Dead" events at various times.
- Bottom Status Bar:** Displays system metrics: "Memory: 136 KBytes", "Sockets: 24", "Events: 260", and control options: "Terminate: Off", "Refuse: Off", "Throttle: ON", "Dangle: Off", "Logging: Off". The time is "9:33 AM".

# ProxyManager Tool

ProxyManager connects to the Internet and downloads lists of proxy servers from various websites

You will have thousands of proxy server IP addresses within minutes

Saves time instead of manually visiting individual web sites looking for free proxy servers





# Super Proxy Helper Tool

Super Proxy Helper will help you to:

- Find anonymous, free, or fastest proxy
- Check proxy status response time within a country
- Determine Proxy type (Transparent, Anonymous, or High anonymity)
- Import export proxy
- Download proxy lists from the web



# Super Proxy Helper Tool (cont'd)

The screenshot shows the 'Super Proxy Helper' application window. The 'Proxy' tab is selected. The 'Proxy Server' section includes a checked 'Use proxy' option, a 'Proxy Server' field containing '65.208.122.46', a 'Port' field containing '3128', and a 'Proxy Country' dropdown menu set to 'UNITED STATES'. There are 'Check' and 'Apply' buttons. Below this is a table of proxy servers with columns for 'Use', 'Server', 'Port', 'Protocol', 'Status', 'Time', 'Type', and 'Country'. The row for '65.208.122.46' is selected. To the right of the table is a vertical stack of buttons: 'Auto-Config', 'Download Proxys', 'Check', 'Check All', 'Stop', 'New', 'Modify', 'Delete', 'Delete All', 'Filtrate', 'Import', 'Export', and 'Config'.

Use	Server	Port	Protocol	Status	Time	Type	Country
<input type="checkbox"/>	201.147.158.52	8080	HTTP	Free	4547	Unknown	MEXICO
<input type="checkbox"/>	200.121.58.71	80	HTTP	Free	1734	Unknown	PERU
<input type="checkbox"/>	84.201.213.245	80	HTTP	Free	-21270	Unknown	POLAND
<input type="checkbox"/>	194.210.66.122	80	HTTP	Free	-18458	Unknown	PORTUGAL
<input type="checkbox"/>	84.235.100.2	8080	HTTP	Free	2047	Unknown	SAUDI ARABIA
<input type="checkbox"/>	84.235.100.2	8080	HTTP	Free	2157	Unknown	SAUDI ARABIA
<input type="checkbox"/>	80.35.163.52	80	HTTP	Free	12844	Unknown	SPAIN
<input type="checkbox"/>	82.198.121.2	8080	HTTP	Free	3829	Unknown	SPAIN
<input type="checkbox"/>	163.30.166.131	80	HTTP	Free	593	Unknown	TAIWAN
<input type="checkbox"/>	220.132.150.147	80	HTTP	Free	22641	Unknown	TAIWAN
<input type="checkbox"/>	81.215.62.232	8080	HTTP	Free	-4990	Unknown	TURKEY
<input type="checkbox"/>	207.71.18.26	80	HTTP	Free	28203	Unknown	UNITED STATES
<input type="checkbox"/>	70.168.187.78	80	HTTP	Free	19391	Unknown	Unknown
<input type="checkbox"/>	129.41.250.20	80	HTTP	Free	23453	Unknown	UNITED STATES
<input checked="" type="checkbox"/>	65.208.122.46	3128	HTTP	Free	22407	Unknown	UNITED STATES
<input type="checkbox"/>	209.203.227.139	80	HTTP	Free	14172	Unknown	UNITED STATES
<input type="checkbox"/>	200.31.137.58	6588	HTTP	Free	3515	Unknown	VENEZUELA
<input type="checkbox"/>	200.93.114.139	8080	HTTP	Free	13469	Unknown	VENEZUELA
<input type="checkbox"/>	201.242.82.210	6588	HTTP	Free	5766	Unknown	Unknown
<input type="checkbox"/>	203.162.89.61	8000	HTTP	Free	2890	Unknown	VIET NAM

# Happy Browser Tool (Proxy-based)

Happy Browser is a multifunctional web browser with many integrated utilities

You can dynamically change proxy servers while browsing the web

You can even use hundreds of proxy servers to browse the web

It is a complete automated proxy-based web browser



# Happy Browser Tool (Proxy-based) (cont'd)

The screenshot shows the 'Proxy Server' window in the Happy Browser application. The window title is 'Proxy Server' and it contains a 'Connect State' section with fields for 'Proxy Server' (82.67.36.5), 'Port' (80), and 'IP'. Below this is a table of proxy servers with columns for 'Use', 'Server', 'Port', 'Protocol', 'Status', 'Time/', 'Type', and 'Country'. The server 82.67.36.5 is selected and checked. To the right of the table are several control buttons: Check, Check All, Stop, New, Modify, Delete, Delete All, Filtrate, Export, Import, Online Import, Config, and Close.

Use	Server	Port	Protocol	Status	Time/	Type	Country
<input type="checkbox"/>	212.0.138.14	80	HTTP	Free	3063	Transparent	SUDAN
<input type="checkbox"/>	221.214.164.52	8080	HTTP	Free	3140	Anonymous	CHINA
<input type="checkbox"/>	209.53.223.129	80	HTTP	Free	4640	Transparent	CANADA
<input type="checkbox"/>	210.99.155.39	8080	HTTP	Free	4672	Transparent	REPUBLIC OF KOREA
<input type="checkbox"/>	217.17.233.188	80	HTTP	Free	5313	Transparent	BAHRAIN
<input type="checkbox"/>	219.166.113.90	3128	HTTP	Free	6344	Transparent	JAPAN
<input type="checkbox"/>	203.187.242.70	80	HTTP	Free	6407	Transparent	INDIA
<input checked="" type="checkbox"/>	82.67.36.5	80	HTTP	Free	6578	Anonymous	FRANCE
<input type="checkbox"/>	212.12.183.55	8080	HTTP	Free	6766	Anonymous	SAUDI ARABIA
<input type="checkbox"/>	212.116.209.234	8080	HTTP	Free	7047	Distorting	SAUDI ARABIA
<input type="checkbox"/>	219.34.121.3	8080	HTTP	Free	7532	Anonymous	JAPAN
<input type="checkbox"/>	217.194.154.129	3128	HTTP	Free	8234	Transparent	NIGERIA
<input type="checkbox"/>	209.236.124.24	8080	HTTP	Free	8547	Transparent	UNITED STATES
<input type="checkbox"/>	203.101.42.91	3128	HTTP	Free	8953	Transparent	INDIA
<input type="checkbox"/>	81.199.108.12	80	HTTP	Free	9187	Transparent	GHANA
<input type="checkbox"/>	202.78.81.3	3128	HTTP	Free	9485	Transparent	PHILIPPINES
<input type="checkbox"/>	200.140.131.194	80	HTTP	Free	11063	Unknown	BRAZIL
<input type="checkbox"/>	203.115.22.83	8000	HTTP	Free	11218	Transparent	SRI LANKA
<input type="checkbox"/>	212.5.193.143	80	HTTP	Free	11281	Anonymous	SLOVAKIA
<input type="checkbox"/>	212.60.65.22	80	HTTP	Free	11344	Anonymous	GAMBIA
<input type="checkbox"/>	80.207.188.140	80	HTTP	Free	12391	Anonymous	ITALY
<input type="checkbox"/>	202.103.234.33	8080	HTTP	Free	12531	Transparent	CHINA
<input type="checkbox"/>	82.129.167.19	3128	HTTP	Free	12719	Transparent	EGYPT
<input type="checkbox"/>	195.175.37.9	8080	HTTP	Free	12969	Transparent	TURKEY

What if your Firewall is blocking you from various proxy servers and anonymizers?

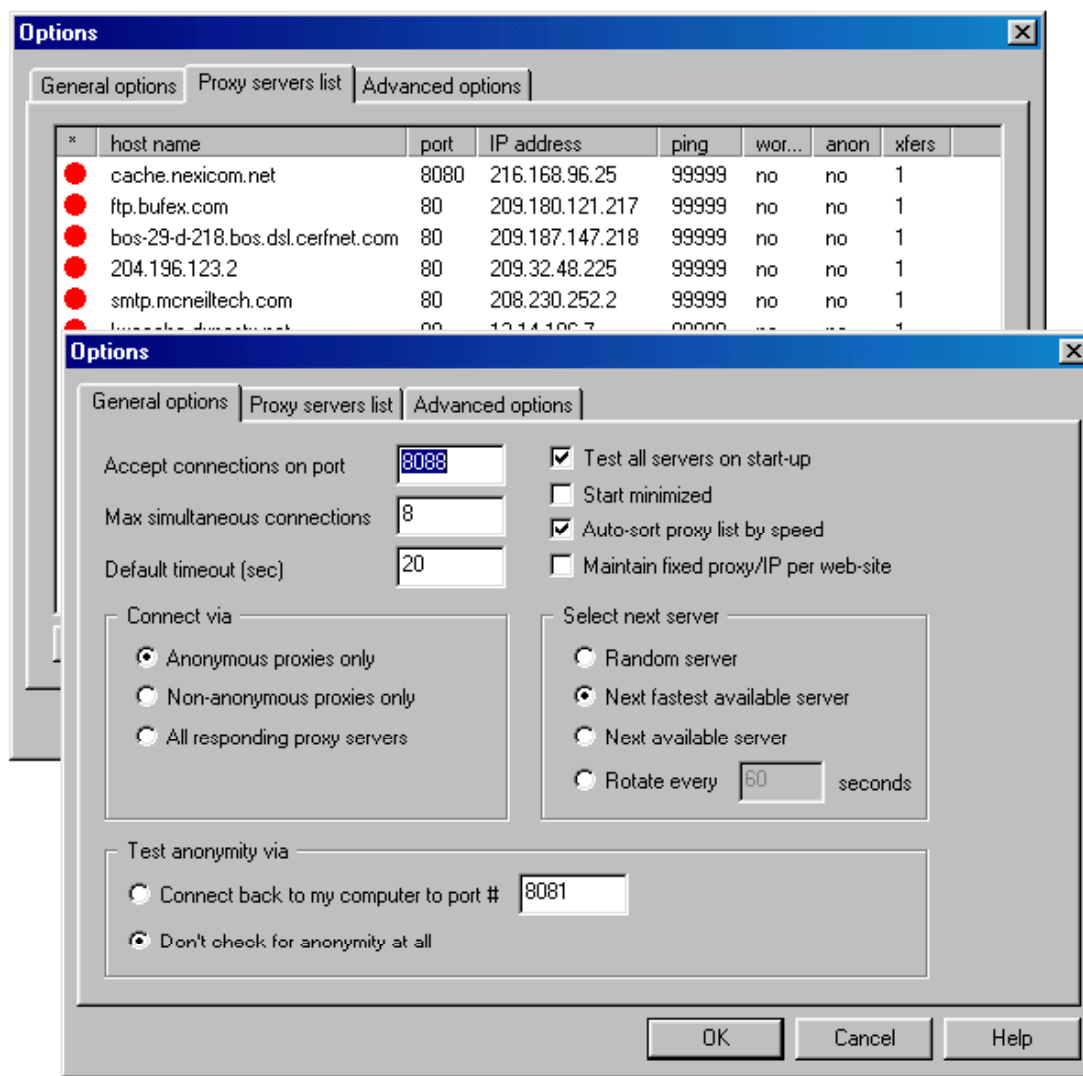
MultiProxy uses different proxies every time you visit the Internet

Add thousands of proxies to the list and your Firewall does not see a pattern in your traffic

This tool can make the trace difficult



# MultiProxy (cont'd)



# How Does MultiProxy Work



**Attacker**

MultiProxy running  
at 127.0.0.1:8088

Every traffic is sent to random proxy in the list

## List of Proxy Servers

```
164.58.28.250:80
194.muja.pitt.washdctt.dsl.att.net:80
web.khi.is:80
customer-148-223-48-114.uninet.net.mx:80
163.24.133.117:80
paubrasil.mat.unb.br:8080
164.58.18.25:80
bpubl014.hgo.se:3128
bpubl007.hgo.se:3128
www.reprokopia.se:8000
193.188.95.146:8080
193.220.32.246:80
Astrasbourg-201-2-1-26.abo.wanadoo.fr:80
gennet.gennet.ee:80
pandora.teimes.gr:8080
mail.theweb.co.uk:8000
mail.theweb.co.uk:8888
194.6.1.219:80
194.79.113.83:8080
ntbkp.naltec.co.il:8080
195.103.8.10:8080
pools1-31.adsl.nordnet.fr:80
pools1-98.adsl.nordnet.fr:80
195.167.64.193:80
server.sztmargitgimi.sulinet.hu:80
los.micros.com.pl:80
195.47.14.193:80
mail.voltex.co.za:8080
196.23.147.34:80
196.40.43.34:80
```



**Target**

**Internet**





# TOR Proxy Chaining Software

Tor is a network of virtual tunnels connected together and works like a big chained proxy

It masks the identity of the originating computer from the Internet

Tor uses random set of servers every time a user visits a site

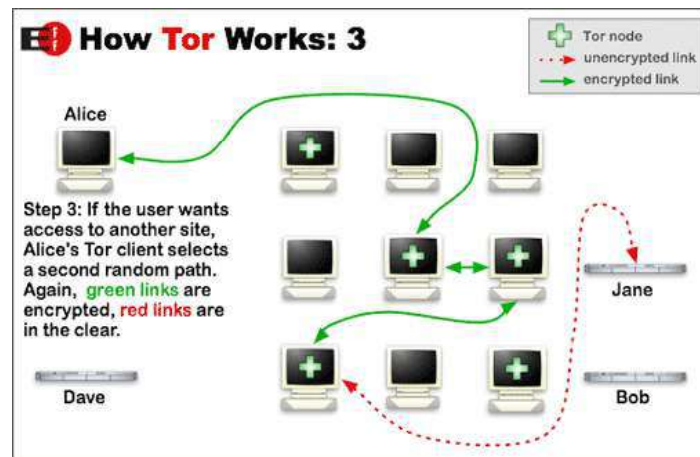
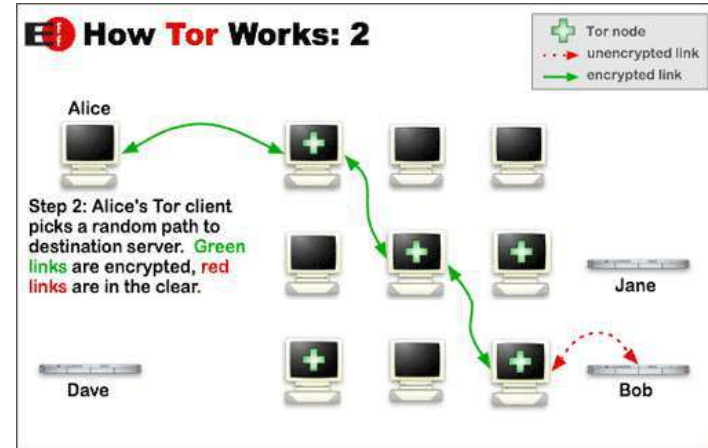
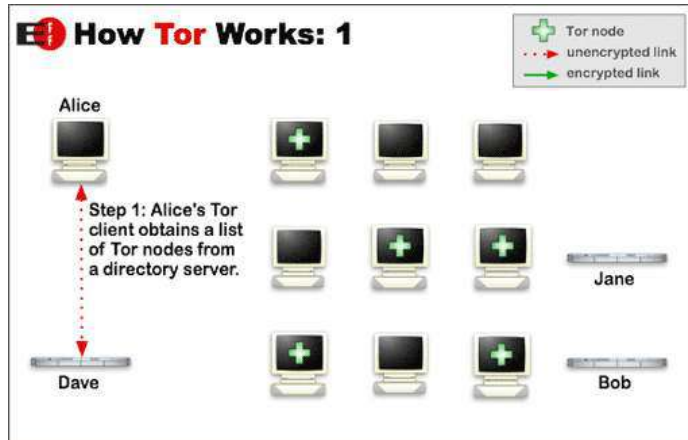
A branch of the U.S. Navy uses Tor for open source intelligence gathering, and one of its teams used Tor while deployed in the Middle East

Law enforcement agencies use Tor for visiting or surveillance of web sites without leaving government IP addresses in their web logs and for security during sting operations

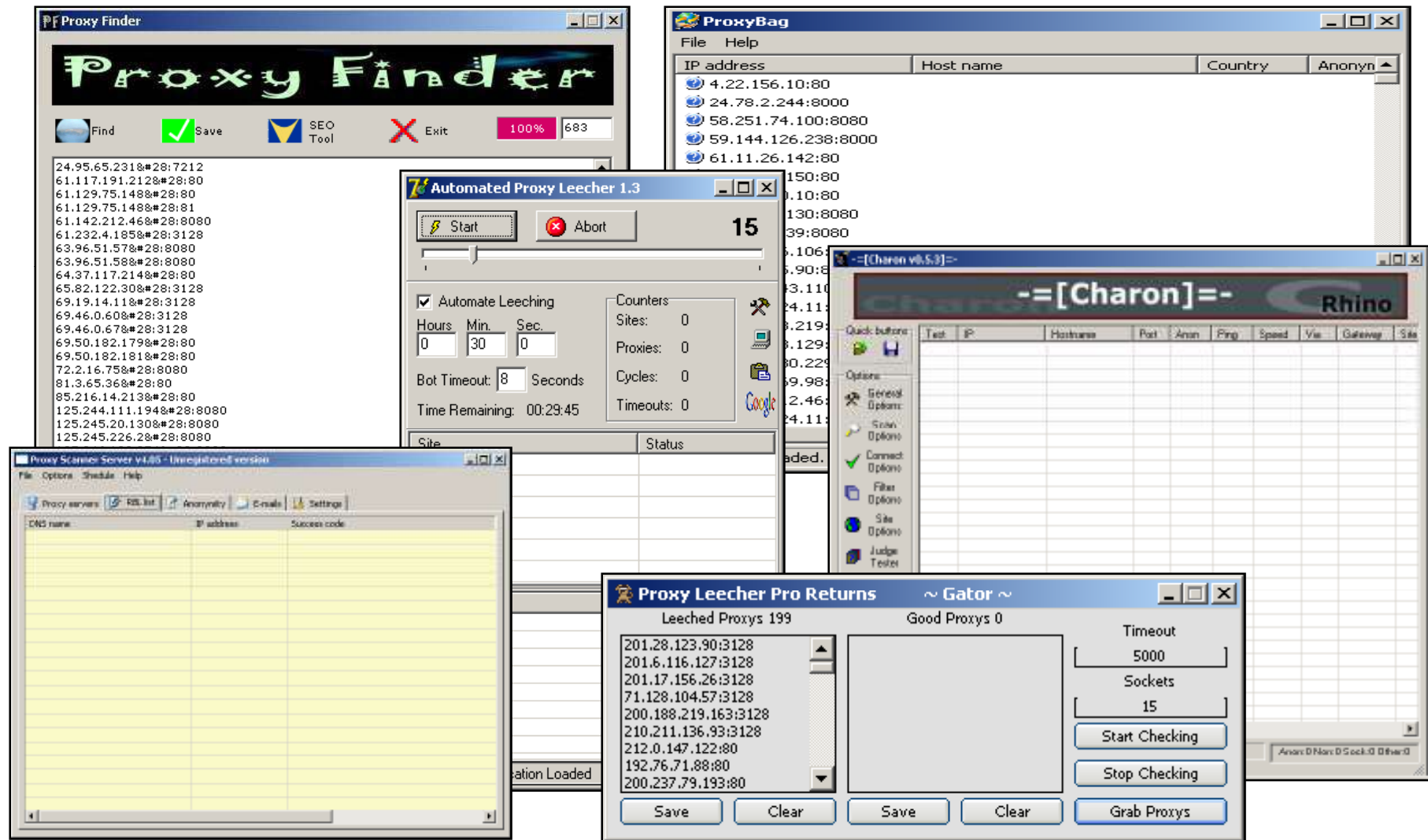
Visit <http://tor.eff.com>



# TOR Proxy Chaining Software



# Additional Proxy Tools



# Anonymizers

Anonymizers are services that help to make web surfing anonymous

The first anonymizer developed was Anonymizer.com, created in 1997 by Lance Cottrell

An anonymizer removes all the identifying information from a user's computers while the user surfs the Internet, thereby ensuring the privacy of the user

## Why Use Anonymizer?

- Example: Google.com keeps track of all your web searches on their servers by placing a cookie on your machine
- Every single search you entered at Google is logged



# Surfing Anonymously



User wants to access  
Sites (e.g. [www.target.com](http://www.target.com)) which have been  
blocked as per company's policy

[www.proxify.com](http://www.proxify.com)

Bypasses the  
security line

Gets access to  
[www.target.com](http://www.target.com)



**Consumer** / **Enterprise**

**Primediuz**  
Digital Privacy

**Member Login**

Products | Support | Privacy Matters | Downloads | About



**Protect Yourself<sup>TM</sup>**

**WebTunnel protects your privacy & identity**

WebTunnel hides your IP to prevent collection of personal information and online activity, and enables access in restricted & blocked networks or countries

**Trusted. Worldwide.**

**WebTunnel Hides & Secures:**

- Web Searches (Google..) & investigations
- Chat, IM & VOIP (Skype, MSN,....)
- File Sharing (Kazaa, Morpheus...)
- Web mail (Hotmail, Yahoo...)
- Newsgroup, online dating, Adult sites
- Wireless activity in any network or Hotspot
- Your own private network VPN
- Against Geo-location, Spyware, keyloggers
- Your Digital Art, research & legal material
- Use on any PC, LAN, WAN, WAP Worldwide
- Break through firewalls, filters & blocking

**Click here** If inside a restrictive network, or state: Iran, China...

**Network Status: OK**

**Evaluation & Promotions**

**Practice Safe Internet** When you shop or search online...( more)

StealthSurfer offers comprehensive protection of personal information, credit card numbers, and financial transactions from online snoops

It is tiny enough to carry on a keychain, and bundled with its own high-speed browser; the USB 2.0 flash drive plugs into the USB port of a Windows XP or Windows 2000 computer and allows users to surf the web with total privacy





# Anonymous Surfing: Browzar

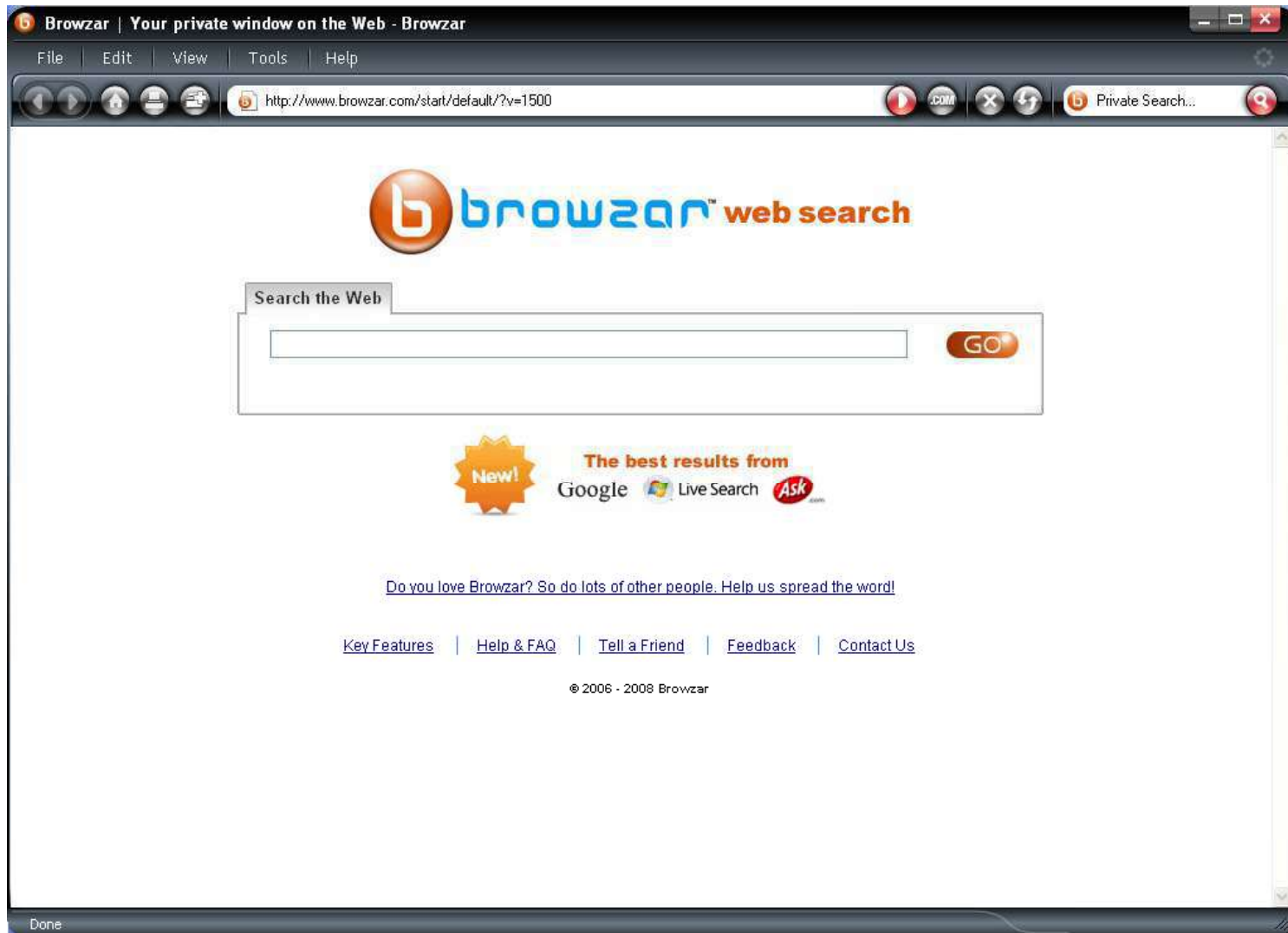


**With Browzar you can search and surf the web without leaving any visible trace on the computer you are using.**

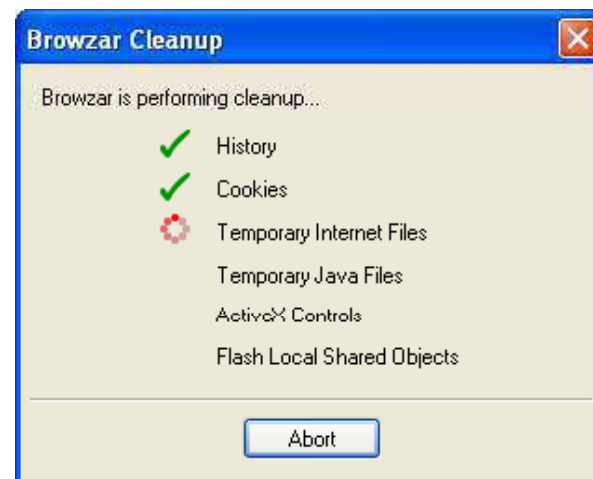
Browzar is based on the Internet Explorer browser engine. Its **free** and only takes seconds to download and you don't even need to install it, so you can download Browzar time and time again, whenever and wherever you need it to protect your privacy.

- ❖ No browsing [history](#), stored files, or [cookies](#)
- ❖ No embarrassing search [auto-complete](#)
- ❖ No installation. Just click 'run' and go
- ❖ No registration required

# Anonymous Surfing: Browzar 1



# Anonymous Surfing: Browzar 2



# Torpark Browser

[www.torrify.com/index.php](http://www.torrify.com/index.php)



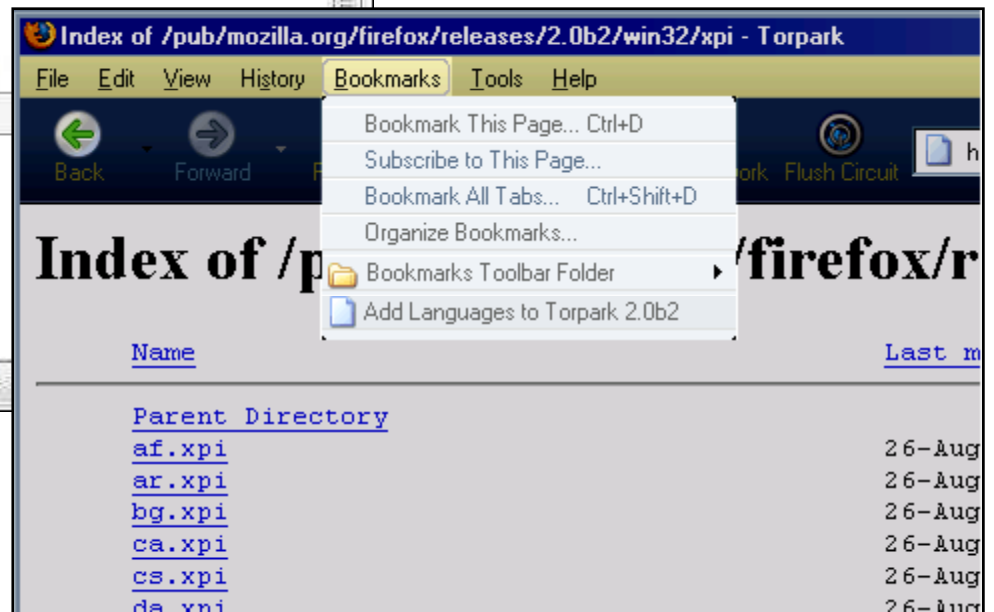
Torpark is free, portable, zero-install, pre-configured, fully anonymous, and encrypted browser which runs on Windows

It is based on the Firefox browser and connects to the Internet via the onion router network



You could even put it on a USB keychain and surf anonymously and leave no tracks behind

# Torpark Browser: Screenshot



GetAnonymous offers a comprehensive online privacy and protection solution that combines several popular features into a single product

## Features:

- Shields your IP address
- Provides you with enhanced proxy suit
- Cleans all traces left on yourpc after surfing the Internet
- Keeps cookies off your computer
- Destroys all logs that may keep information about your surfing habits
- Controls data going out of your computer
- Blocks data sent to you by a suspicious server
- HTTP, HTTPS, SOCKS4, and SOCKS5 support
- Logs all your surfing activities
- Controls your level of privacy with customized settings



# GetAnonymous: Screenshots 1

The image displays two overlapping screenshots of the GetAnonymous v2.0 application interface. The top-left window shows the 'General Settings' section, which includes a 'Server Port' field set to 8082 and a 'Server Type' dropdown menu set to HTTP. Below this, the 'Other Settings' section contains two unchecked checkboxes: 'Autostart GetAnonymous' and 'I'm Behind a Firewall'. At the bottom of this window, there is an IP address field (127.0.0.1), a 'Port' field (80), and a 'Type' dropdown menu (HT). The bottom-right window shows the 'Privacy' settings, with 'IP Shielding (Connect Using Proxy Chain)' checked. Underneath, 'Use one Proxy' is selected, with 'Choose best proxy' as the chosen option. There is also an option for 'Let Me Select Proxy' with associated IP and Port fields. At the bottom, 'Use Proxy Chain' is unselected, with fields for 'Chain Length' (0) and 'Time To Change' (1) Mins. Both windows feature a navigation sidebar on the left with buttons for 'General Settings', 'Advanced Settings', 'Proxy Tools', 'Activity Logs', and 'Help', along with 'Apply Changes' and 'Exit Program' buttons at the bottom.



# GetAnonymous: Screenshots 2

**GetAnonymous v2.0**  
The Unidentified Experience

**Proxy Capture** | **Proxy Analyzer**

Captured Programs

Program Name	Protocol Type
--------------	---------------

**GetAnonymous v2.0**  
The Unidentified Experience

**Privacy** | **Filtration** | **Windows Cleaner**

Auto clean on browser exit |  Auto clean on program exit  
 Auto clean on windows start

**Clean Now**

**System Cleaner**

**Menus**

- Run History
- Find Computer
- Clear Network connections
- Telnet History
- Last Login
- Find Files

**Folders**

- Recycle Bin
- Temp Folder
- Recent Folder

**Select All**

**IE Cleaner**

IP Privacy is a privacy protection tool that hides your computer IP address preventing your surfing habits and your Internet activity over the Internet from being tracked by websites or Internet Service Providers

IP Privacy provides a good online privacy protection by cleaning all online traces that may harm or use inadvertently information on your computer:

- Clears Internet History
- Clears Typed URL
- Clears Temporary Internet Files
- Clears Cookies
- Clears Auto Complete Forms History
- Clears Auto complete Password History
- Clears Internet Favorites



# IP Privacy: Screenshot

The screenshot shows the IP Anonymizer web application. The interface has a blue header with the text "ip anonymizer" and a red shield icon. On the right side of the header, there are "update now" and "help" links. A left sidebar contains buttons for "status", "anonymity", "privacy", "settings", and "register". The main content area is titled "select a proxy" and features two dropdown menus: "New" and "Tested". The "New" dropdown is open, showing a list of proxy servers with their IP addresses and locations. The "Tested" dropdown is currently empty. Below the dropdowns, there are two large buttons: "Disable Online Anonymity" (with a red 'X' icon) and "Enable Privacy" (with a green checkmark icon). At the bottom of the main area, the "status" section displays "Mode: TRIAL COPY", "Status: Online Anonymity: Enabled" (in green), and "Privacy: Disabled" (in red). A link "click here" is provided for more information. The footer of the application shows the "Real IP Address: 192.168.1.6" and the "Current IP Address in use: 130.60.48.211:3124->Switzerland". A "check ip now" button is located in the bottom right corner.

**select a proxy**

**New**

- 130.60.48.211:3124->Switzerland
- 130.60.48.211:3124->Switzerland
- 130.88.203.26:3128->UK
- 139.19.142.4:3128->Germany
- 195.116.60.1:3128->Poland
- 193.63.75.18:3124->UK
- 192.38.109.143:3128->Denmark
- 141.24.33.161:3124->Germany

**Tested**

- 130.60.48.211:3124->Switzerland

Choose a proxy from the Tested list that includes proxies you have already tested during one session of using IP Anonymizer

**Disable Online Anonymity**

**Enable Privacy**

**status**

Mode: TRIAL COPY  
Status: Online Anonymity: **Enabled**  
Privacy: **Disabled**  
To learn more about Anonymity and Privacy [click here](#)

Real IP Address:192.168.1.6  
Current IP Address in use: 130.60.48.211:3124->Switzerland

check ip now

# Anonymity 4 Proxy (A4Proxy)

[www.inetprivacy.com](http://www.inetprivacy.com)

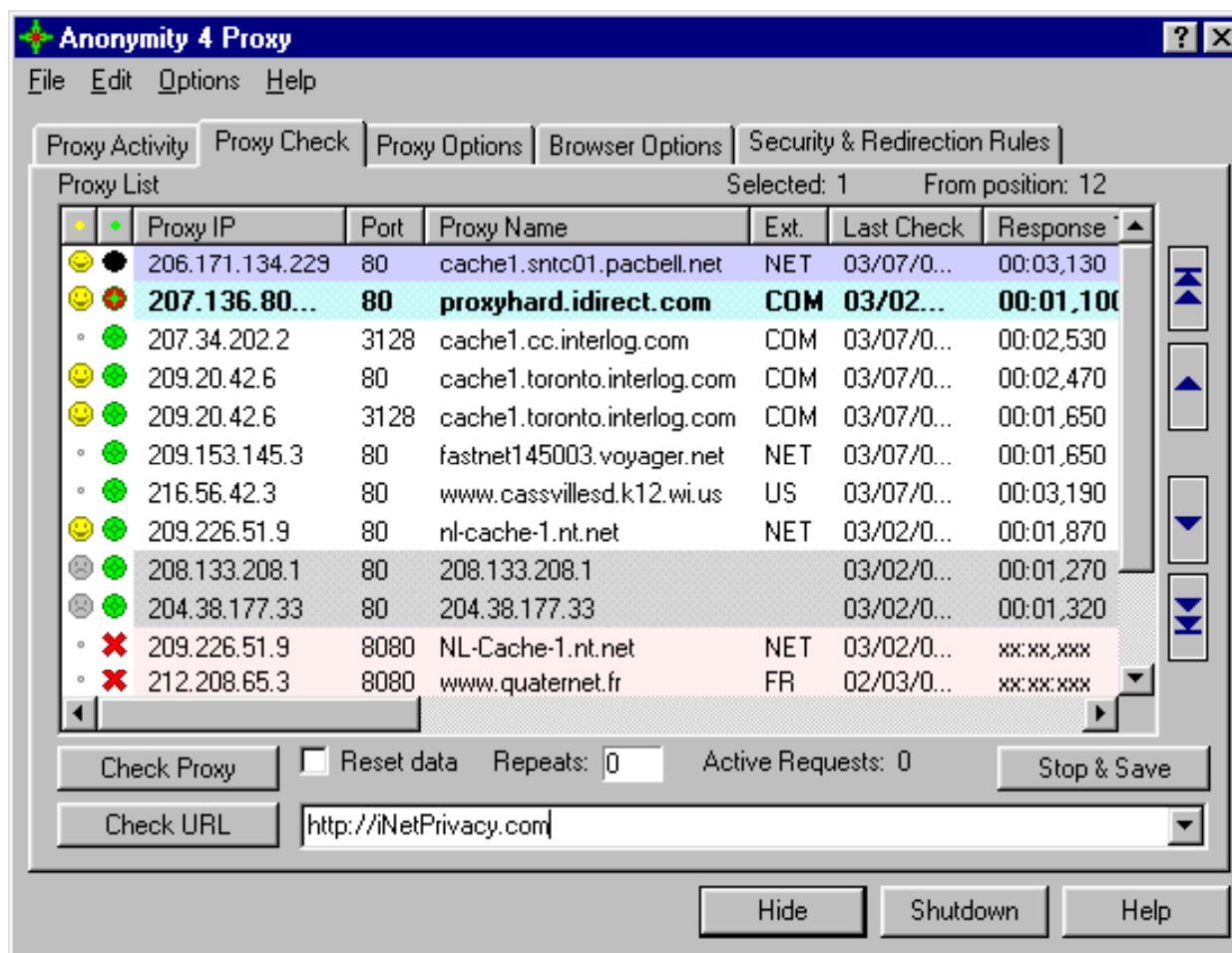
A4Proxy is a personal anonymous proxy server and anonymizing software

This local proxy server includes a database with hundreds of anonymous public proxy servers located all over the world

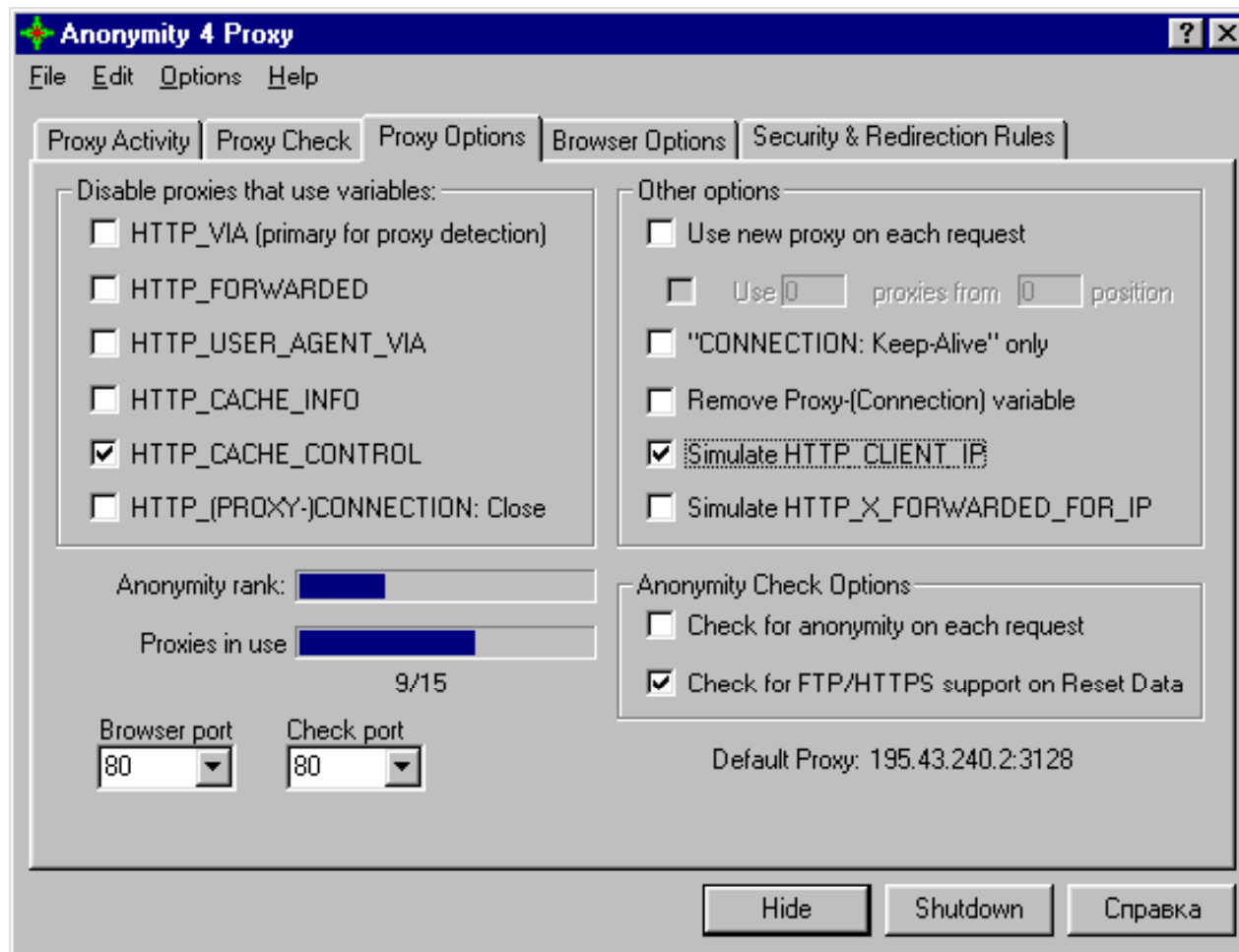
## Benefits:

- Visits any website in the world without telling them who you are and where you live
- Optionally modifies the operating system and other technical information sent out by your browser
- Confuses the websites further by sending them a fake IP address along with your requests
- Downloads files with programs like GetRight and other download managers staying anonymous to the sites from which you download
- If you are a webmaster, submit multiple webpages to search engines without having to worry about submission limits - submit each page using a different anonymous proxy!

# Anonymity 4 Proxy: Screenshot 1



# Anonymity 4 Proxy: Screenshot 2



# Anonymity 4 Proxy: Screenshot 3

The screenshot shows the 'Anonymity 4 Proxy' application window. The title bar reads 'Anonymity 4 Proxy' with a help icon and a close button. The menu bar includes 'File', 'Edit', 'Options', and 'Help'. Below the menu bar are several tabs: 'Proxy Activity', 'Proxy Check', 'Proxy Options', 'Browser Options', and 'Security & Redirection Rules'. The 'Proxy Activity' tab is active, displaying a table of sockets activity. Above the table, it shows 'Sockets activity:' and 'Sockets used: 6' with a progress indicator. The table has columns for #ID, Status, Received, Sent, Proxy IP, Port, and Client. Below the table are two lists: 'Proxy Clients:' containing '127.0.0.1' and 'Requested Hosts:' containing 'microsoft.com', 'm.doubleclick.net', 'ad.doubleclick.net', 'hg1.hitbox.com', and '209.75.21.6'. At the bottom of the window are three buttons: 'Hide', 'Shutdown', and 'Help'.

#ID	Status	Received	Sent	Proxy IP	Port	Client
0	Received	351	825	209.20.42.6	80	127.0.0.1
1	Connect			209.20.42.6	80	127.0.0.1
2	Sent	408	825	209.20.42.6	80	127.0.0.1
3	Sent	787	1219	209.20.42.6	80	127.0.0.1
4	Closed by Remote	17123	277	209.75.22.131	80	127.0.0.1
5	Closed by Remote	7339	257	209.75.22.131	80	127.0.0.1

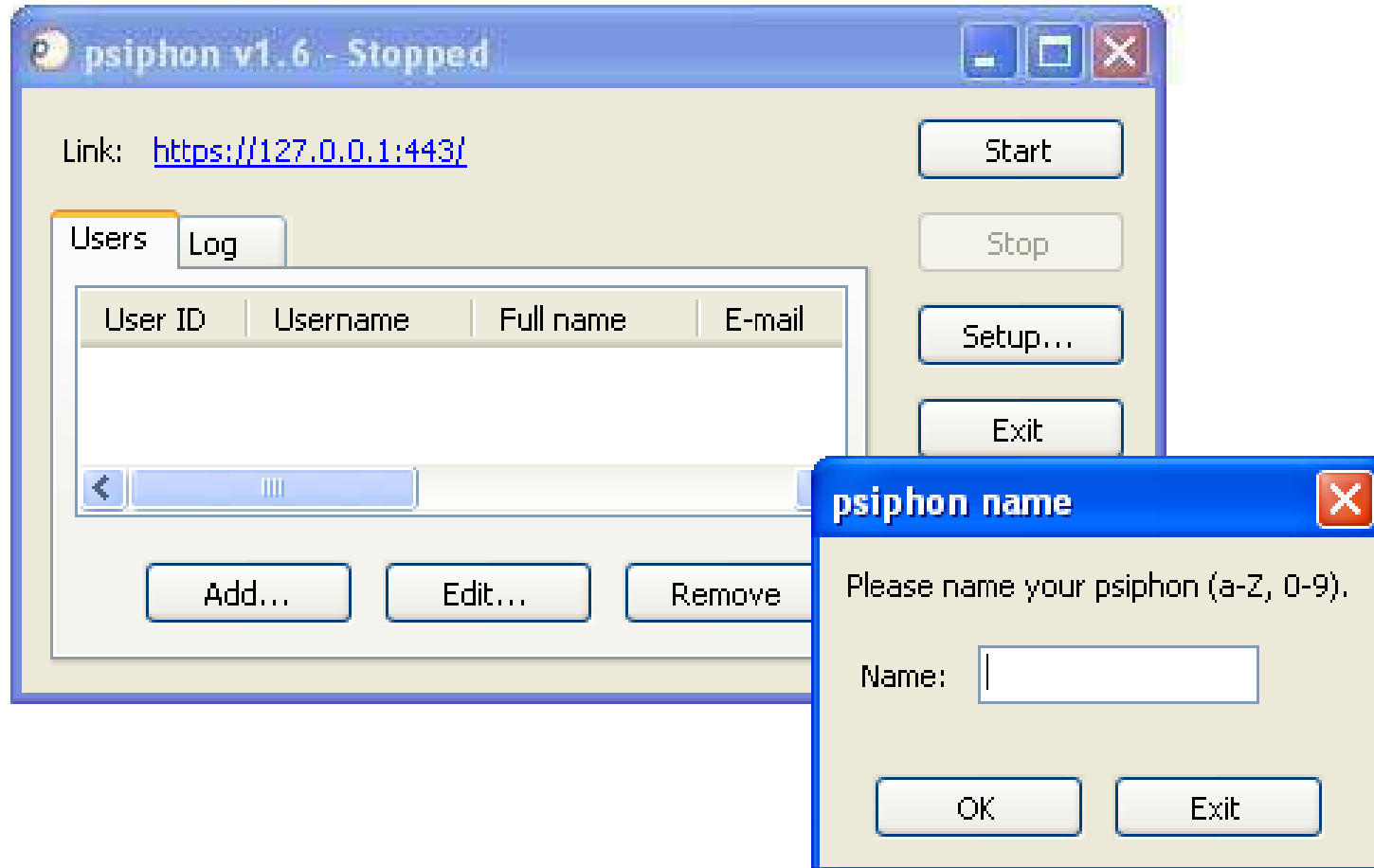


Psiphon is a human rights software project developed by the Citizen Lab at the Munk Centre for International Studies

It allows citizens in uncensored countries to provide unfettered access to the Net

They can access with their home computers to friends and family members who live behind firewalls of states that censor

# Psiphon: Screenshot



# Connectivity Using Psiphon

uncensored country



WIKIPEDIA  
*Die freie Enzyklopädie*

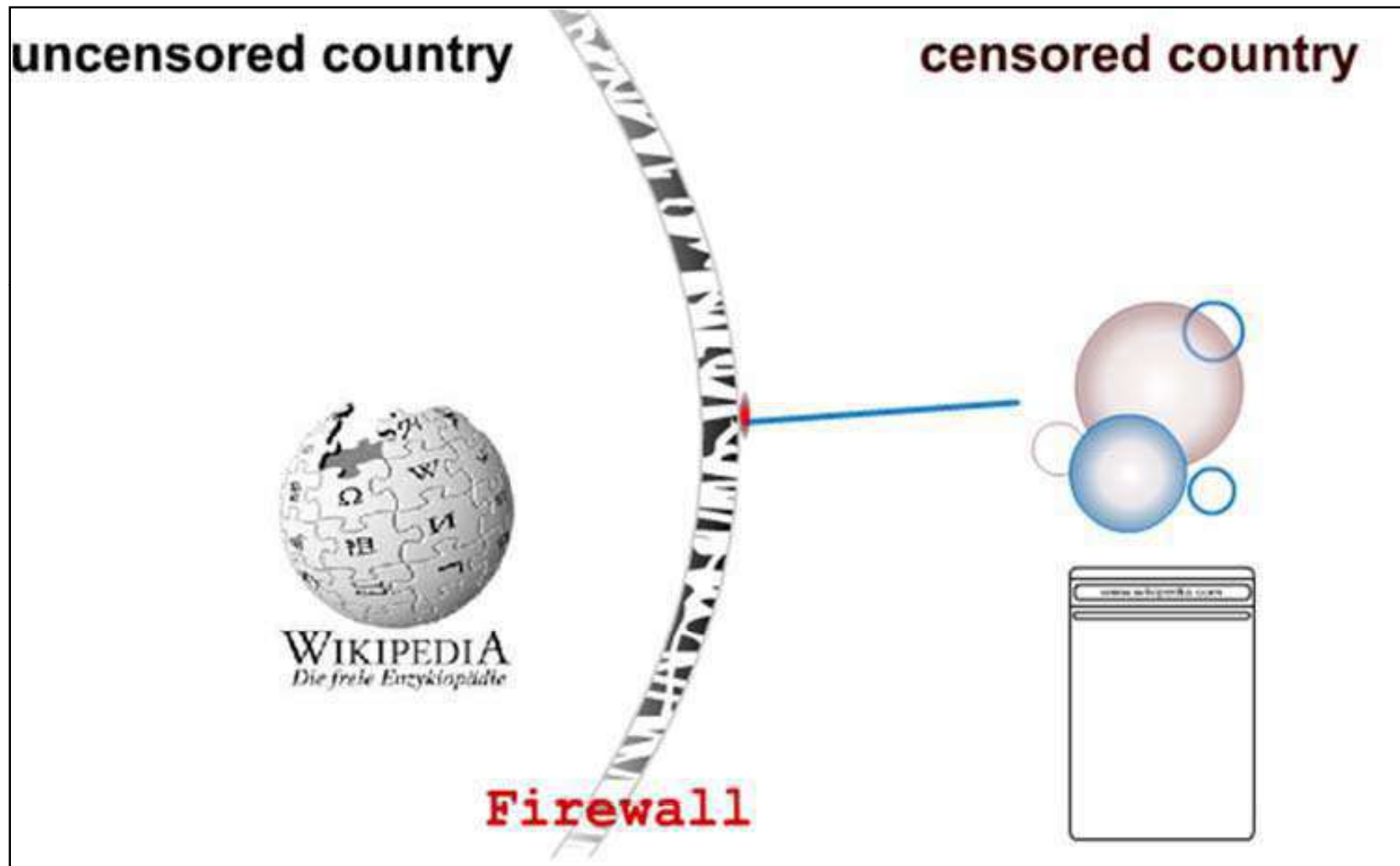
**Firewall**

censored country

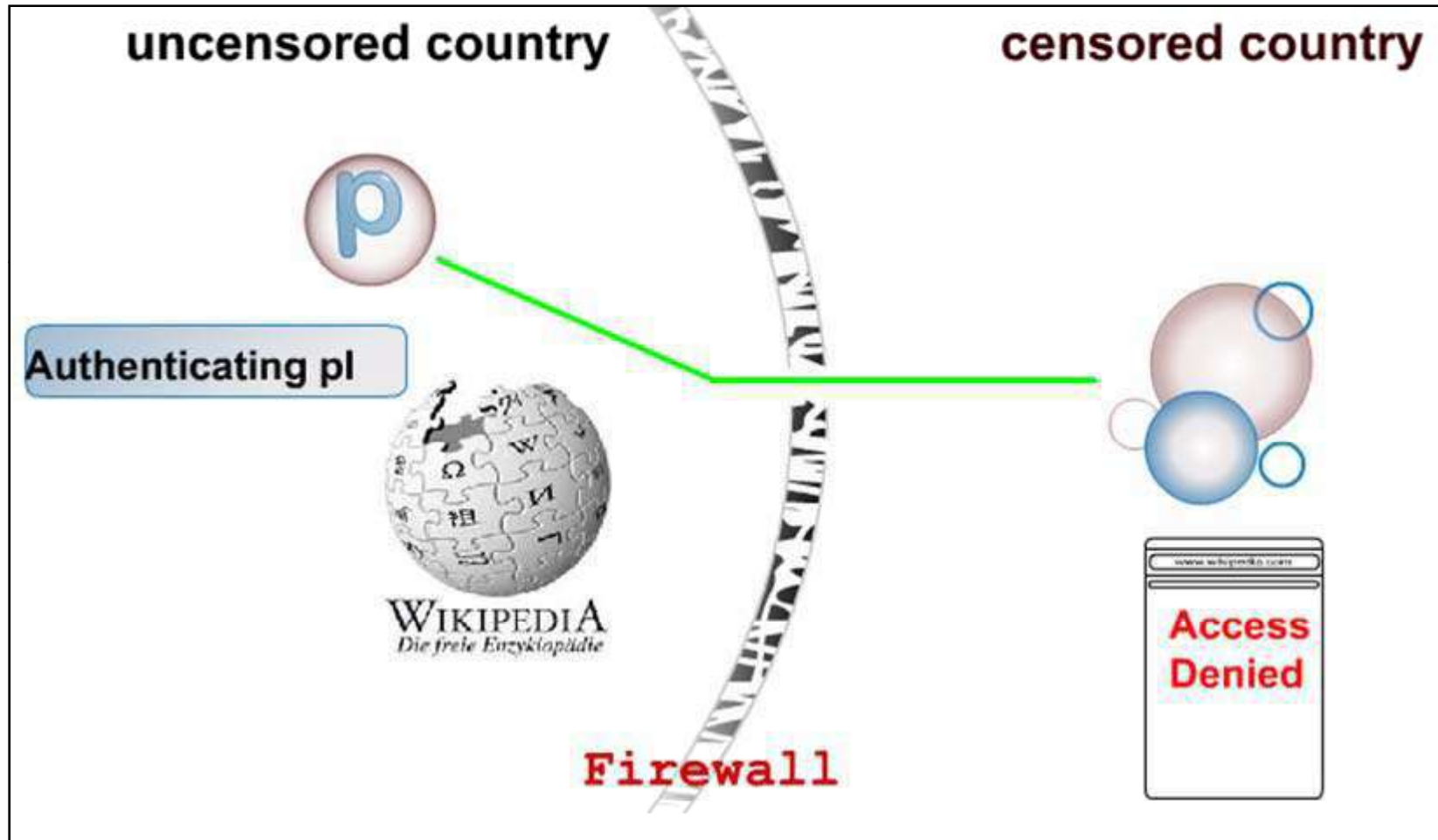
Connect to Wikipedia



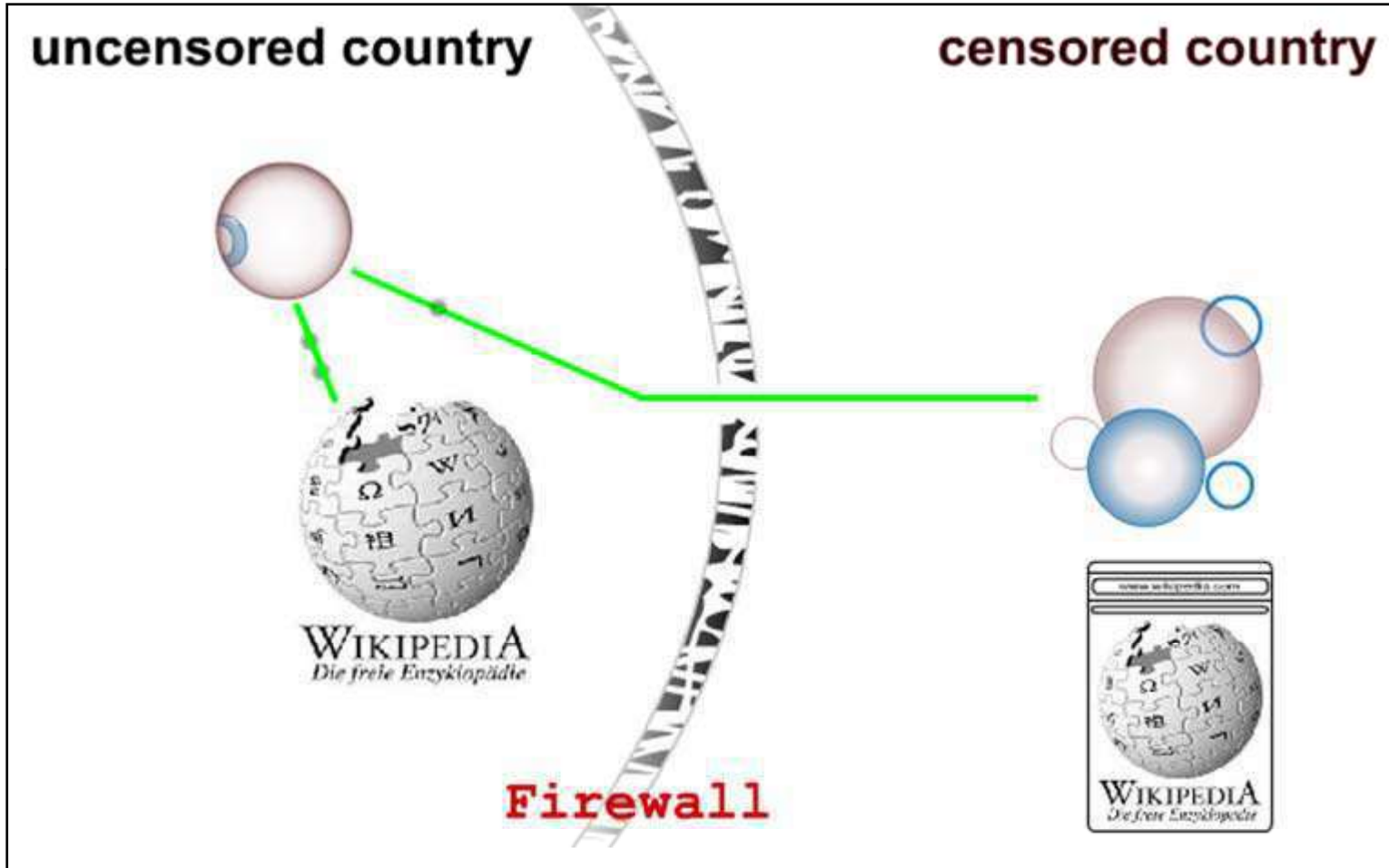
# Connectivity to Wikipedia – Step 1



# Connectivity to Wikipedia – Step 2



# Connectivity to Wikipedia – Step 3



# Bloggers Write Text Backwards to Bypass Web Filters in China

Bloggers and journalists in China are using a novel approach to bypass Internet filters in their country – they write backwards or from right to left

The content therefore remains readable by human beings but defeats the web filtering software

China is known to implement ‘packet filtering’ – a technique that detects TCP packets containing controversial keywords like Tibet, Democracy, Tiananmen, etc

To dodge these censors, Internet writers in China are writing backwards when posting to web forums and blogs

They do it using this web tool that flips sentences to read right to left instead of left to right, and vertically instead of horizontally



Dismissing privacy concerns, a judge ordered YouTube to disclose who watches which video clips and when.



w  
h  
e  
n  
c  
l  
i  
p  
s  
a  
n  
d  
i  
h  
v  
i  
d  
e  
o  
w  
a  
t  
c  
h  
e  
s  
w  
h  
o  
c  
l  
o  
s  
e  
t  
h  
e  
s  
e  
v  
i  
d  
e  
o  
s  
Y  
o  
u  
T  
u  
b  
e  
d  
i  
s  
c  
l  
o  
s  
e  
t  
o  
Y  
o  
u  
T  
o  
r  
A  
j  
u  
d  
g  
e  
o  
r




# Vertical Text Converter

<http://www.cshbl.com/gushu.html>

Vertical text converter

[A netizen asked city posters column Home](#)

This tool can be converted into ordinary text Hengpai classical Shupai from right to left manner, and to increase the appropriate standard line for readers. You can Forum, to speak before the blog tool to use this article to be published by the conversion, and then paste it to be published by the Forum, blog boost. This can be an effective procedure to prevent the site search filtering of certain terms, and without prohibition to read. That is, promote the Chinese classical culture, has also increased interest. Try not fast. [By Ctrl + D BOOKMARK](#)

 [Browser can be directly converted vertical text!](#)  [You no longer need to find this page. to copy to a copy.](#)  [New tools simpler, more quickly, the vertical text more easily.](#)

卍 = 卍 = 卍 = 卍 = 卍 = 卍 || | Bo and the || | || || not show off | | former |, | || || nuisance | | on the use and | | this || | | to hir

1, you want to convert the text input to the input box below

2, click the button 'conversion'

Per page  Vertical lines, each vertical line  The use of the word  Border  Traditional conversion  [Copy conversion results](#)  Not to increase the converter information

3, the result below, you can copy to the group, the blog to the inside

# How to Check If Your Website Is Blocked In China or Not

"How do I find out if web users in China can access my website at xyz.com?"

If you get a "Packets lost" error or there is a time-out while connecting to your site, chances are that the site is restricted

1. Just Ping - They have checkpoints inside Hong Kong and Shanghai in China

- <http://www.just-ping.com/index.php>



2. Watch Mouse - This service too has monitoring stations inside Hong Kong and Shanghai in China

- <http://www.watchmouse.com/en/ping.php>



3. Website Pulse - In addition to Hong Kong and Shanghai, Website Pulse conducts website connectivity test from a computer located in Beijing as well

- <http://www.websitepulse.com/help/testtools.china-test.html>

# Mowser and Phonifier

Surf the web using Mowser and Phonifier, a new service that is free and converts any website into a mobile phone friendly format

[www.mowser.com](http://www.mowser.com)

[www.phonifier.com](http://www.phonifier.com)



Go!

- feeds
- free games!
- directory
- tech 100
- politics 100
- searches

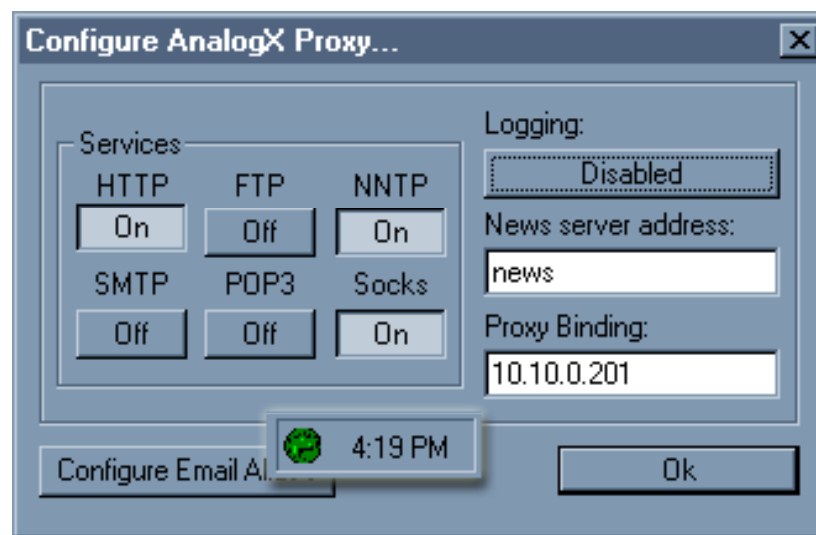
about

© dotMobi 2007-2008. All rights reserved

# AnalogX Proxy

AnalogX Proxy is a small and simple server that allows any other machine on your local network to route it's requests through a central machine

Supports HTTP (web), HTTPS (secure web), POP3 (receive mail), SMTP (send mail), NNTP (newsgroups), FTP (file transfer), and Socks4/4a and partial Socks5 (no UDP) protocols



NetProxy is a secure, reliable, and highly cost-effective method of providing simultaneous Internet access to multiple network users with only one Internet connection of almost any type

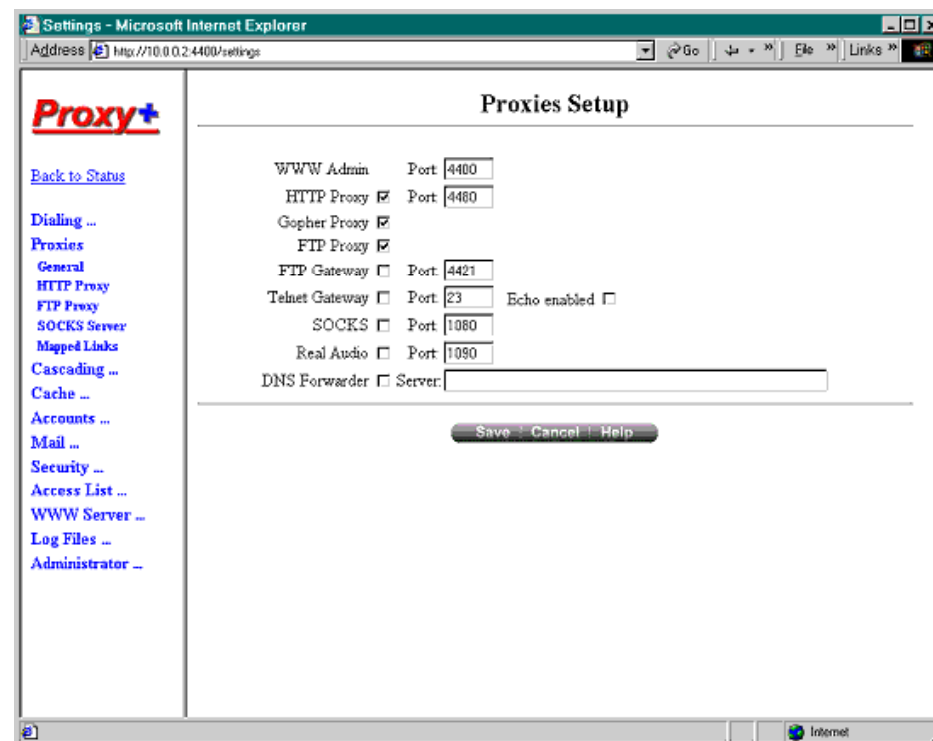




Proxy+ works as firewall proxy server and mail server

### Features:

- Separates the LAN from the Internet to protect from attacks
- Insecure interfaces (connected to the internet) are detected automatically
- Cache increases speed of data retrieval and enables the use of data even if a connection is not established
- Sends and receives mail for many Internet mail boxes at one time using the POP3 protocol
- Full SMTP mail server for one or more domains
- Option for leaving messages on POP3 server





ProxySwitcher Lite is a handy tool to quickly switch between different proxy servers while surfing the Internet

## Features:

Change proxy settings on the fly

Automatic proxy server switching for anonymous surfing

Works with Internet Explorer, Firefox, Opera, and others

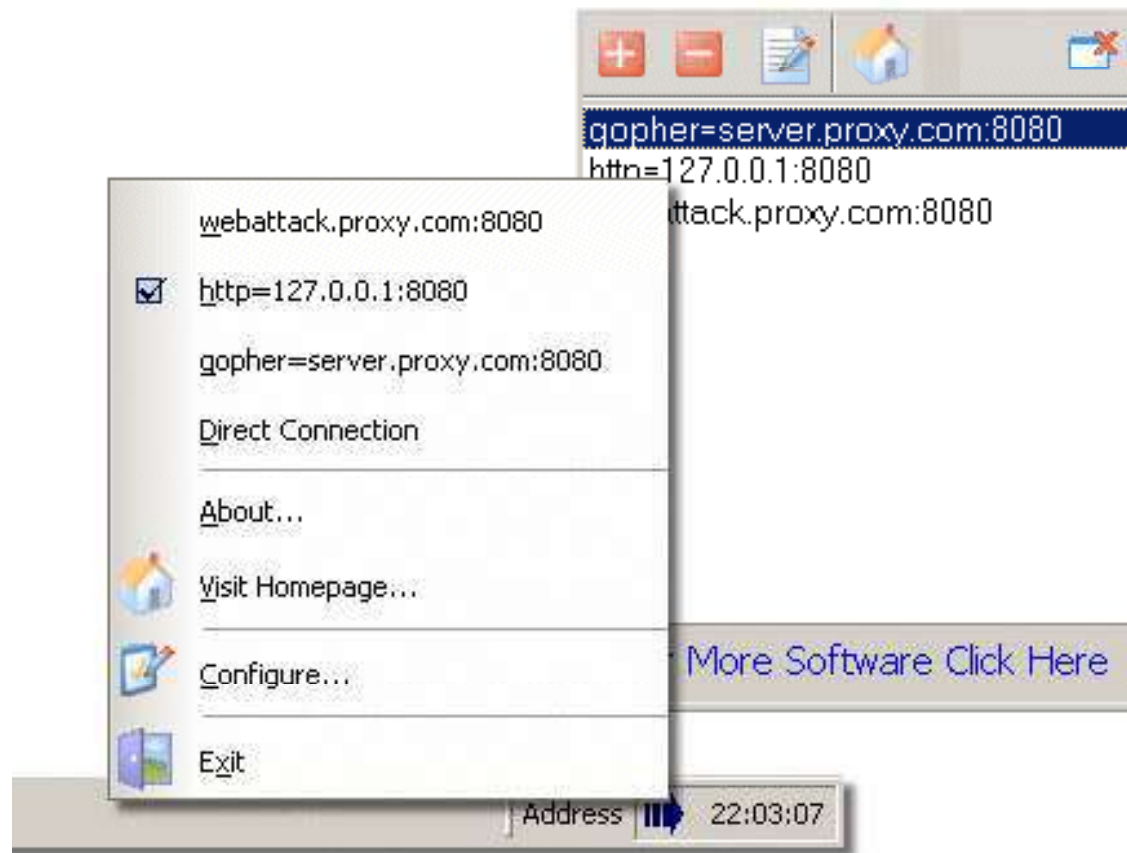
Flexible proxy list management

Proxy server availability testing

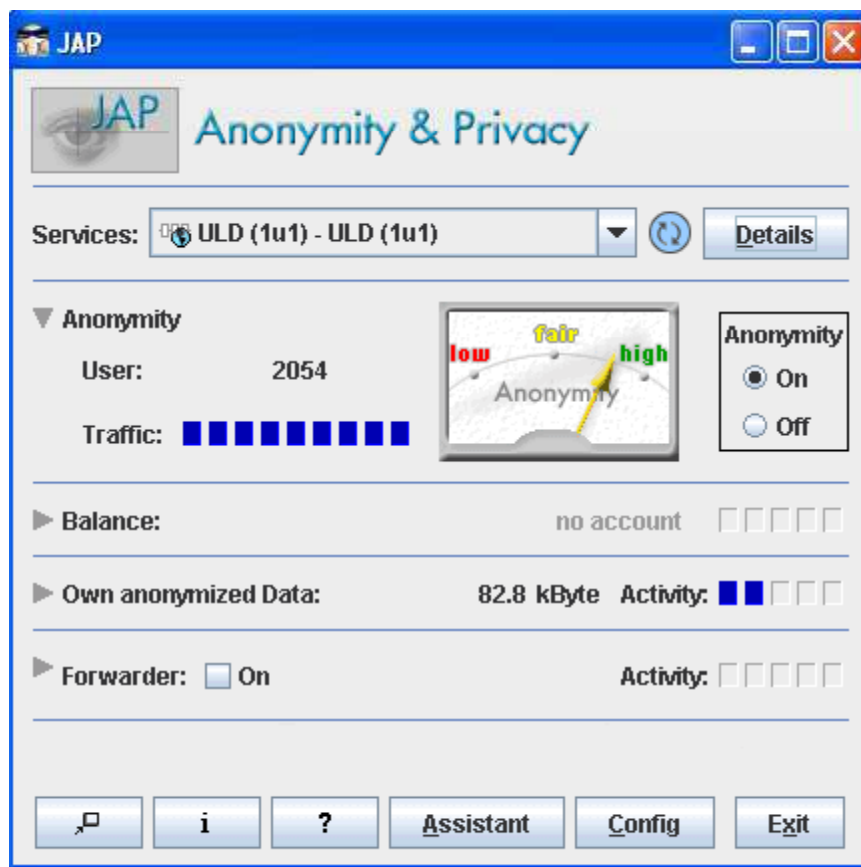
Anonymous proxy server list download



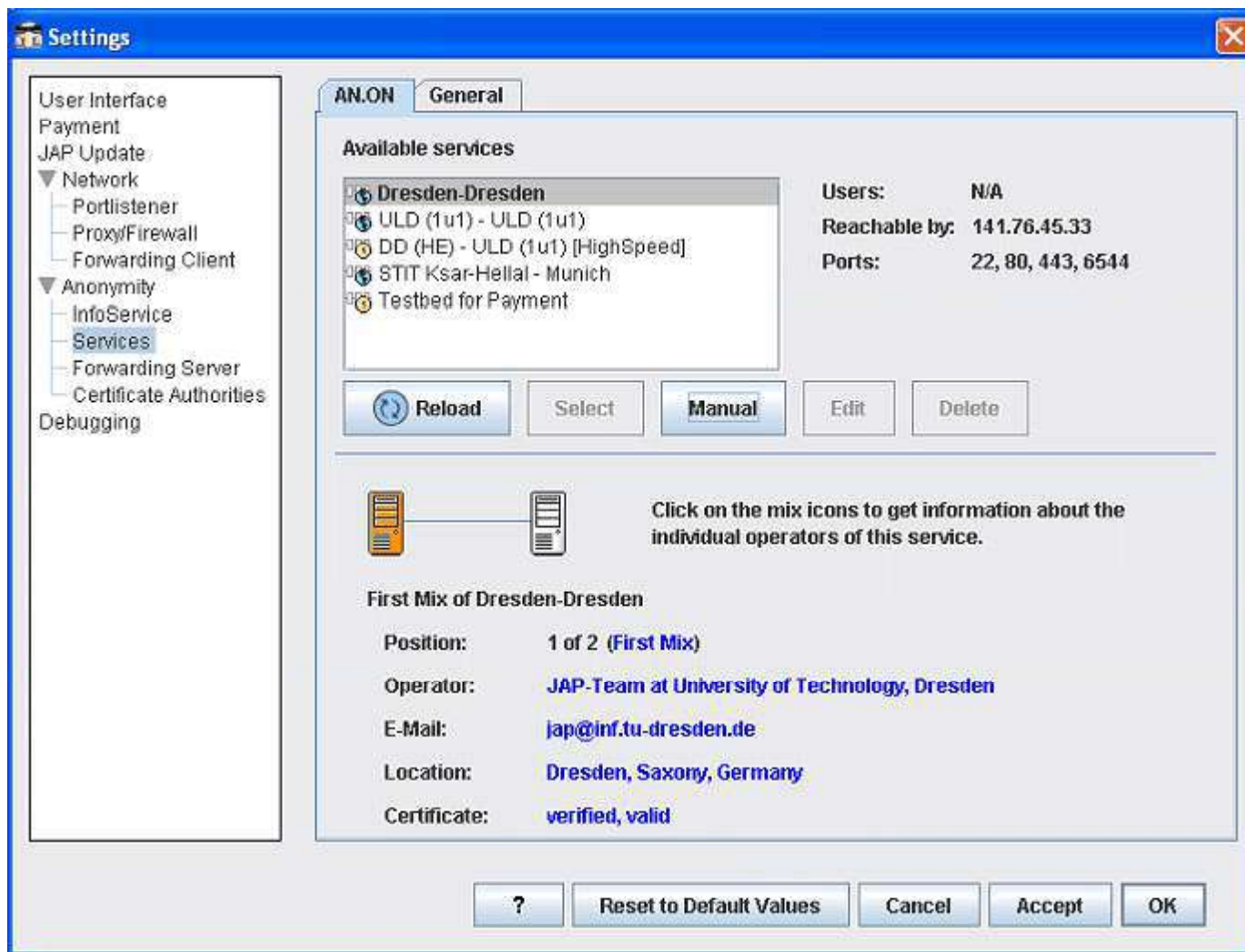
# ProxySwitcher Lite: Screenshot



JAP enables anonymous web surfing with any browser through the use of integrated proxy services that hide your real IP address



# JAP: Screenshot



Proxomitron is a flexible HTTP web filtering proxy that enables to filter web content in any browser

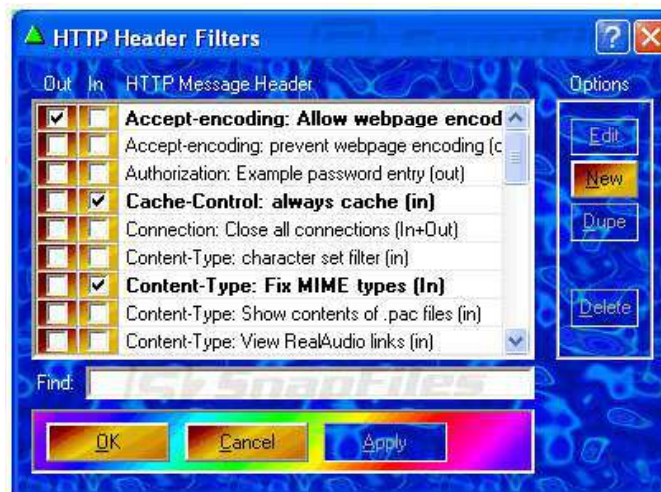
This program runs as a local proxy server and needs to configure browser to use a local host at port 8080 in order to activate filtering

Proxomitron allows you to remove and replace ad banners, Java scripts, off-site images, Flash animations, background images, frames, and many other page elements

HTTP headers can be added, deleted, or changed

Proxomitron filters can be customized and edited as per needs

# Proxomitron: Screenshots





# Google Cookies

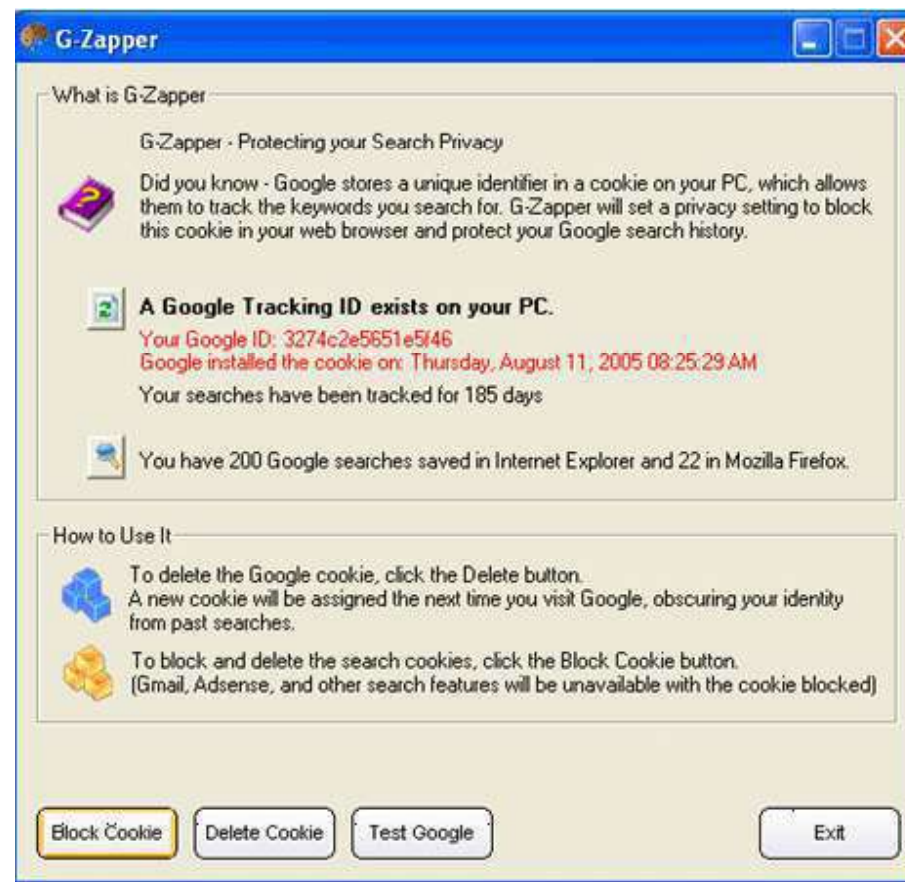
"Google builds up a detailed profile of your search terms over many years. Google probably knew when you last thought you were pregnant, what diseases your children have had, and who your divorce lawyer is."  
BBC technology commentator Bill Thompson

G-Zapper helps you stay anonymous while searching Google by deleting or blocking the Google cookie that tracks your preferences and search history

*This is what Google's log might look like when you search for "cars"*



```
inktomil-lng.server.ntl.com - 25/Mar/2003 10:15:32  
http://www.google.com/search?q=cars" - MSIE 6.0; Windows NT 5.1 -  
740674ce2123e969 ← PRIVACY COOKIE
```





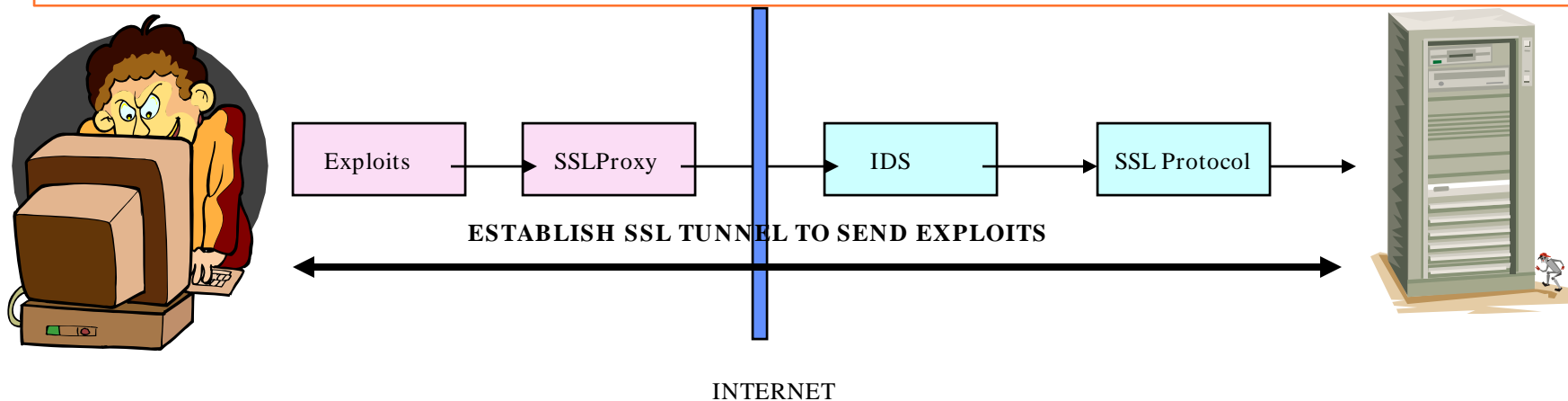
# SSL Proxy Tool

SSLproxy is a transparent proxy that can translate between encrypted and unencrypted data transport on socket connections

It also has a non-transparent mode for automatic encryption-detection on netbios

## When should I use SSLProxy?

- Let's say you want to launch an attack on a remote server which has SSL installed
- The exploits you send will be caught by the IDS and you want to mask this detection
- Run SSLproxy on your machine and tunnel all the exploits through this proxy, which will use SSL to transmit the packets to the remote server blinding the IDS



# How to Run SSL Proxy

Window 1: Client – Hacker Machine Run:

- `sslproxy -L127.0.0.1 -l55 -R <some remote IP> -r 443 -c dummycert.pem -p ssl2`

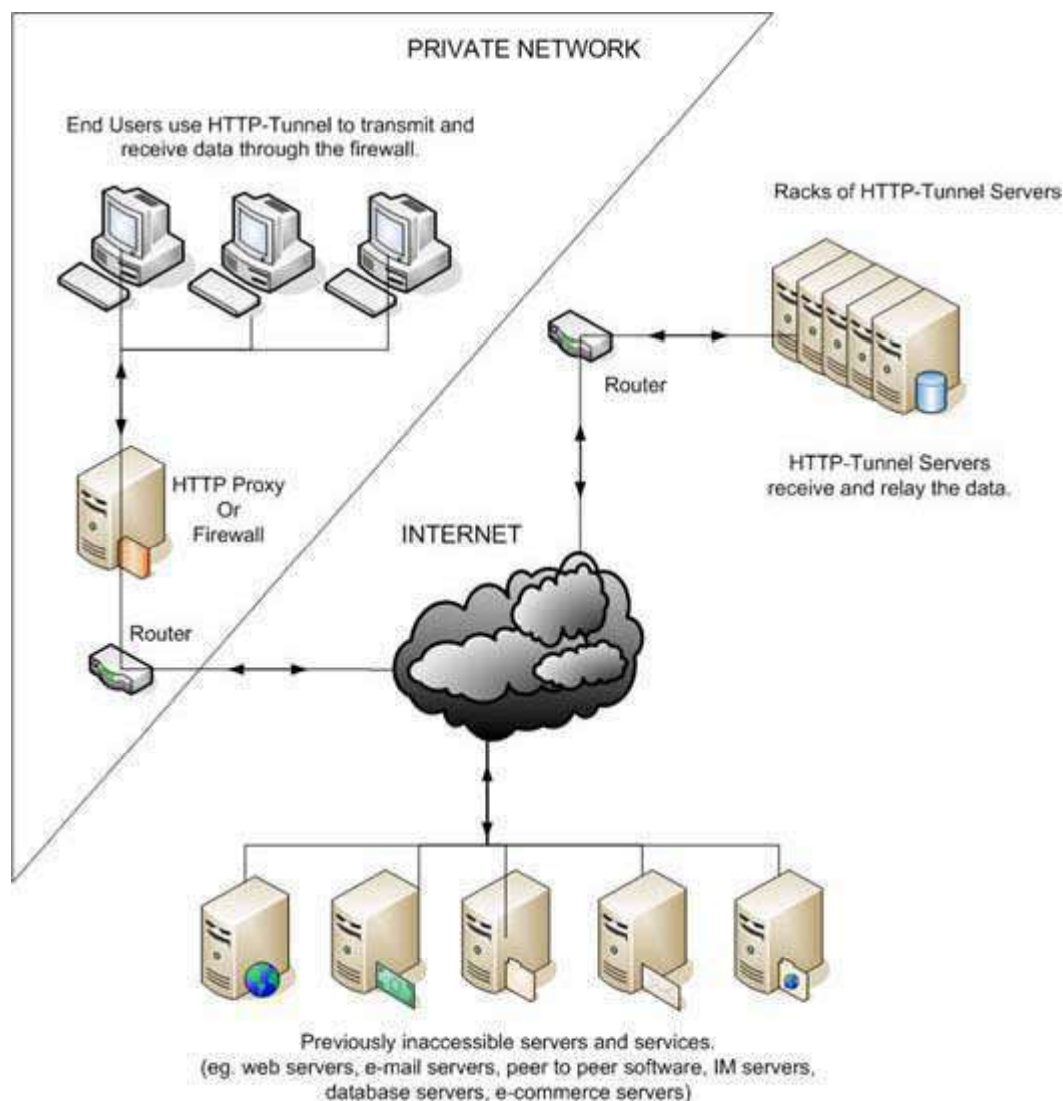
Window 2: Client - Connect to 127.0.0.1 port 55 and send your exploits

- Example: `telnet 127.0.0.1 55`
- Then type `GET /`

```
C:\WINDOWS\System32\cmd.exe - sslproxy -L127.0.0.1 -l55 -R 64.90.176.10 -r 443 -c dummycert.pem -p ssl2
^C
J:\Ethical Hacking and Countermeasures v5\Module 03 - Scanning\sslproxy\sslproxy
_native_windows\Release>sslproxy -L127.0.0.1 -l55 -R 64.90.176.10 -r 443 -c dumm
ycert.pem -p ssl2
proxy ready, listening for connections
connection on fd=1920
SSL: No verify locations, trying default
SSL: Cert error: unknown error 20 in /C=US/O=Equifax Secure Inc./CN=Equifax Secu
re Global eBusiness CA-1
SSL: negotiated cipher: DES-CBC3-MD5
client: broken pipe (read)
jumping catch
```

```
Command Prompt
C:\Documents and Settings\Haja>telnet localhost 55
```

# HTTP Tunneling Techniques



HTTP Tunneling technology allows users to perform various Internet tasks despite the restrictions imposed by firewalls

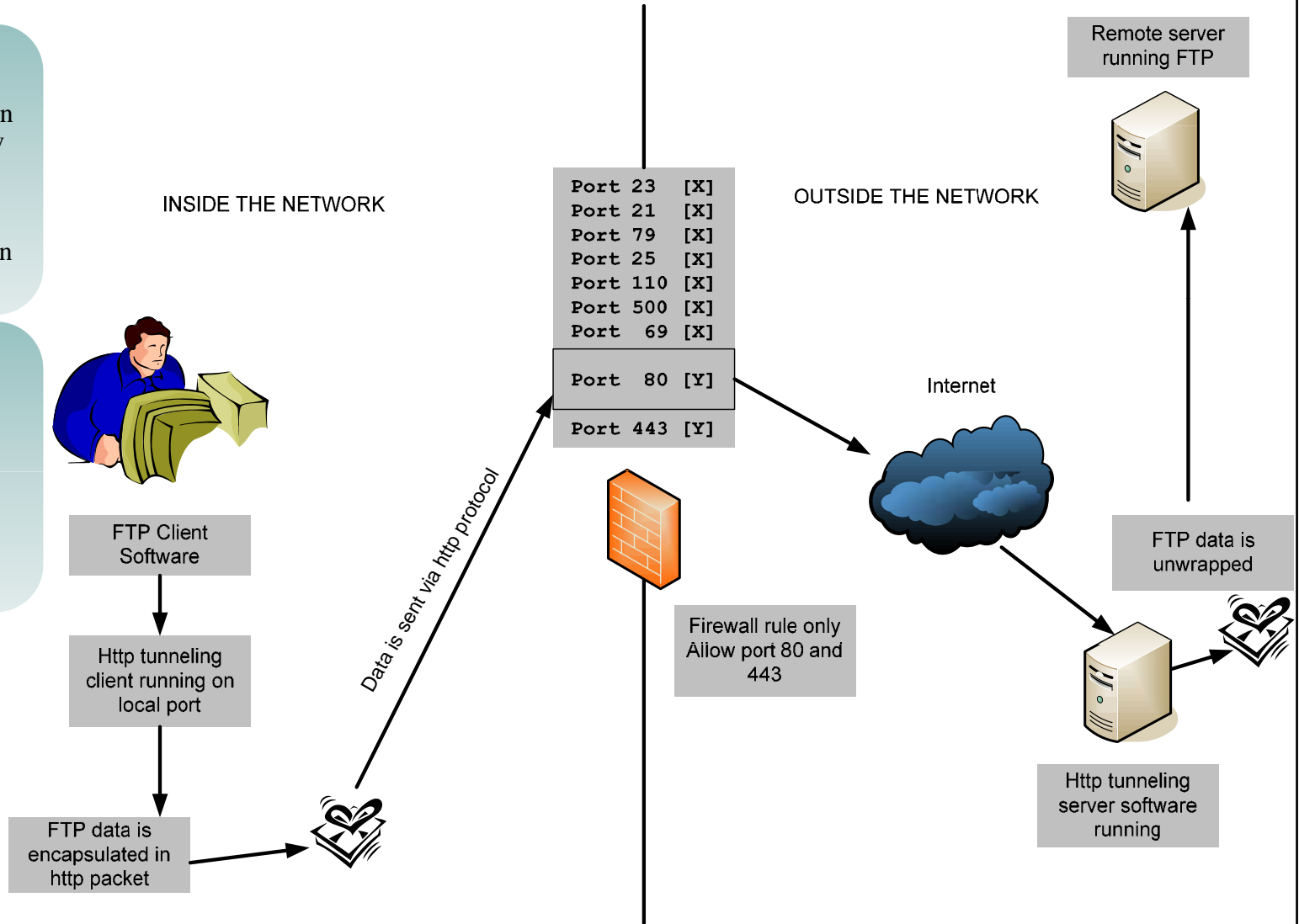
This is made possible by sending data through HTTP (port 80)



# Why Do I Need HTTP Tunneling

Let's say your organization has blocked all the ports in your firewall and only allows port 80/443 and you want to use FTP to connect to some remote server on the Internet

In this case, you can send your packets via http protocol





httpunnel creates a bidirectional virtual data connection tunnelled in HTTP requests. The HTTP requests can be sent via an HTTP proxy if so desired

This can be useful for users behind restrictive firewalls

If WWW access is allowed through an HTTP proxy, it is possible to use httpunnel and, say, telnet or PPP to connect to a computer outside the firewall

**On the server you must run hts. If I wanted to have port 80 (http) redirect all traffic to port 23 (telnet) then it would go something like:**

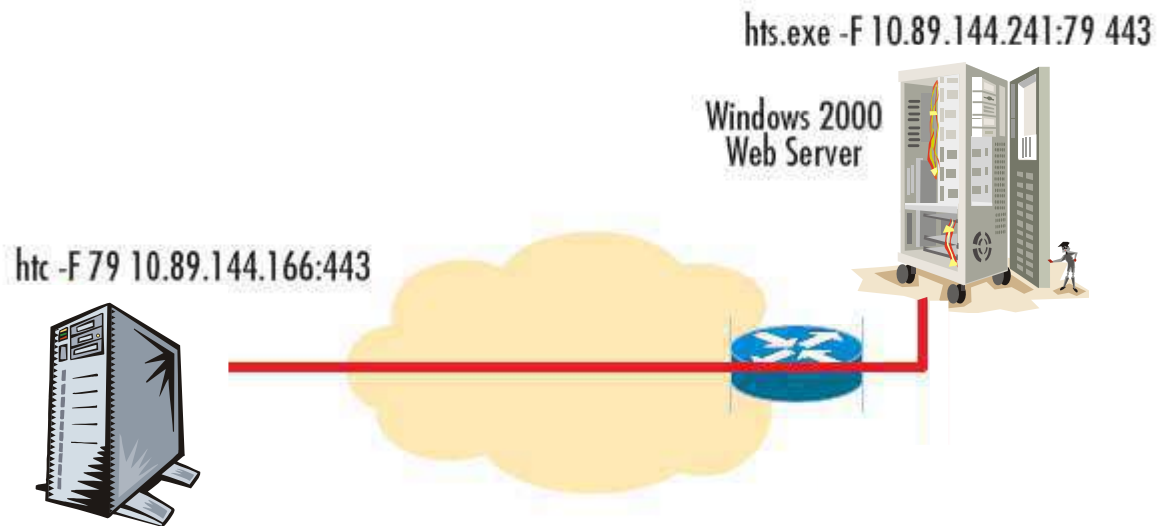
```
hts -F server.test.com:23 80
```

**On the client you would run htc. If you are going through a proxy, the -P option is needed otherwise omit it.**

```
htc -P proxy.corp.com:80 -F 22 server.test.com:80
```

Then telnet localhost and it will redirect the traffic out to port 80 on the proxy server and on to port 80 of the server, then to port 23.

# How to Run Httpptunnel



HTTP-Tunnel acts as a socks server allowing you to use your Internet applications safely despite restrictive firewalls and gives you an extra layer of protection against hackers, spyware, and ID theft's

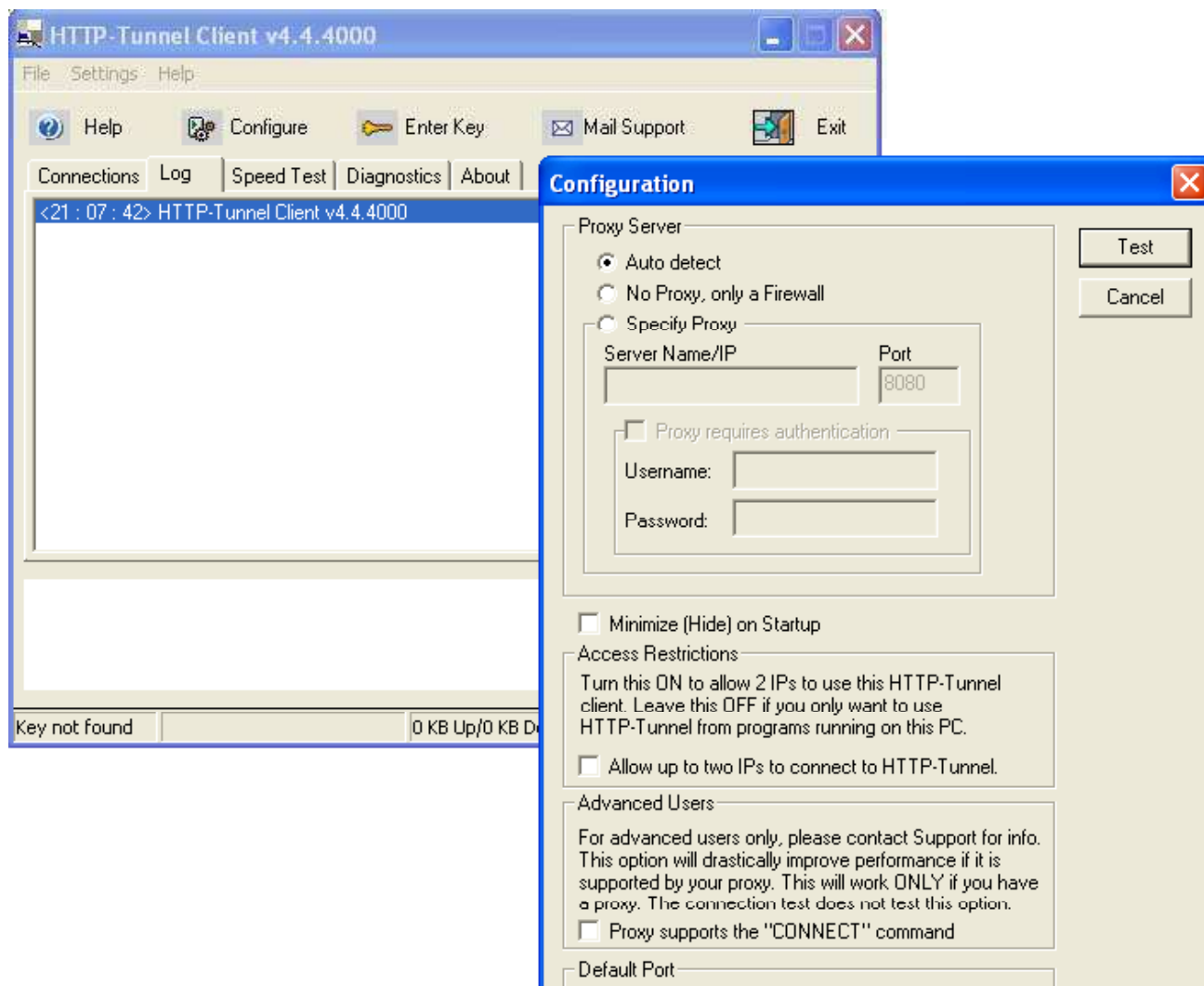
## Features:

- Bypasses any firewall
- Secures Internet browsing
- Can use favorite programs without being monitored
- Has extra security for online transactions
- Encrypts all your Internet traffic
- Visits sites that were previously blocked
- Prevents 3rd party monitoring or regulation of your Internet browsing and downloads
- Uses your favorite applications previously blocked
- Hides your IP address

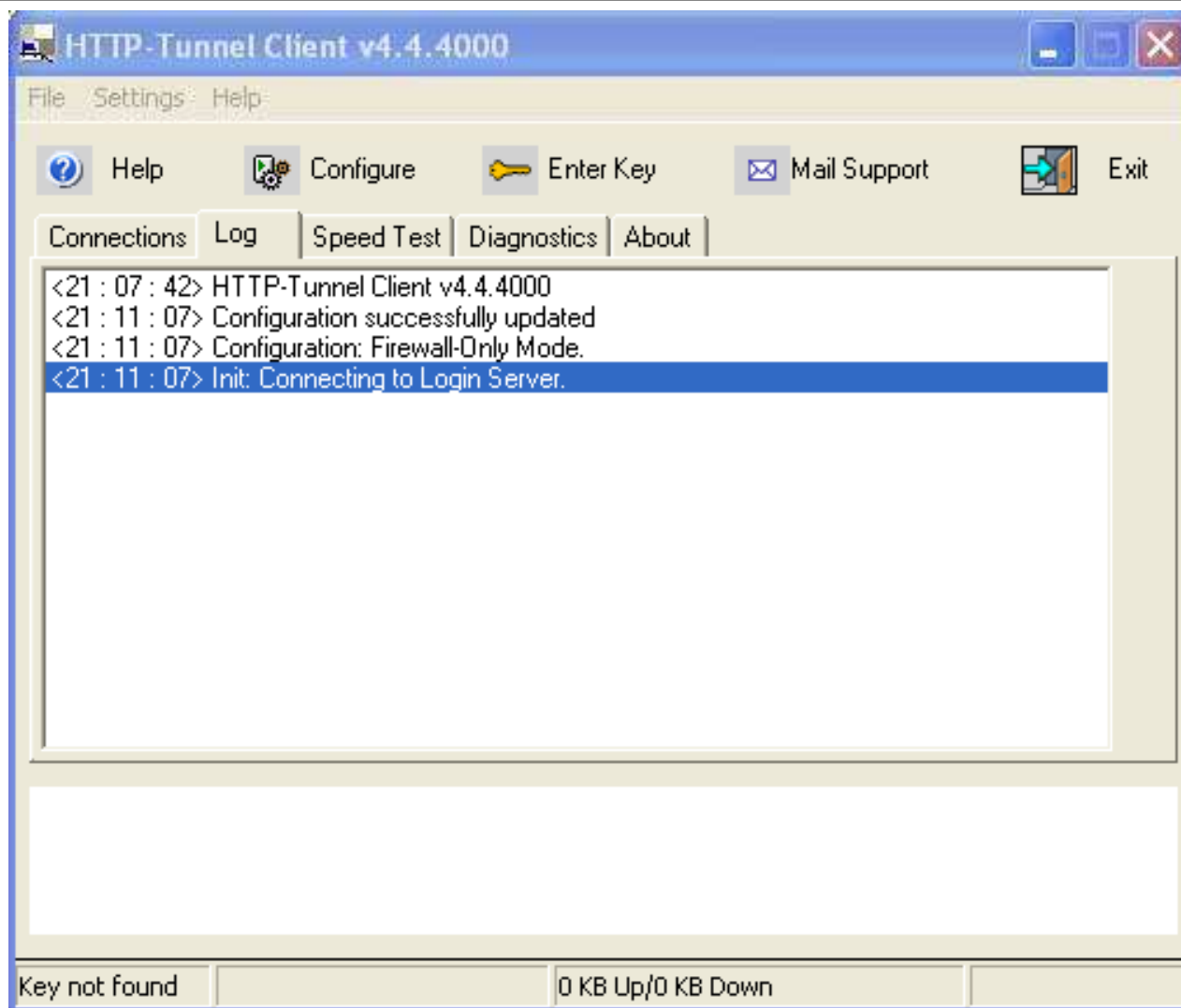




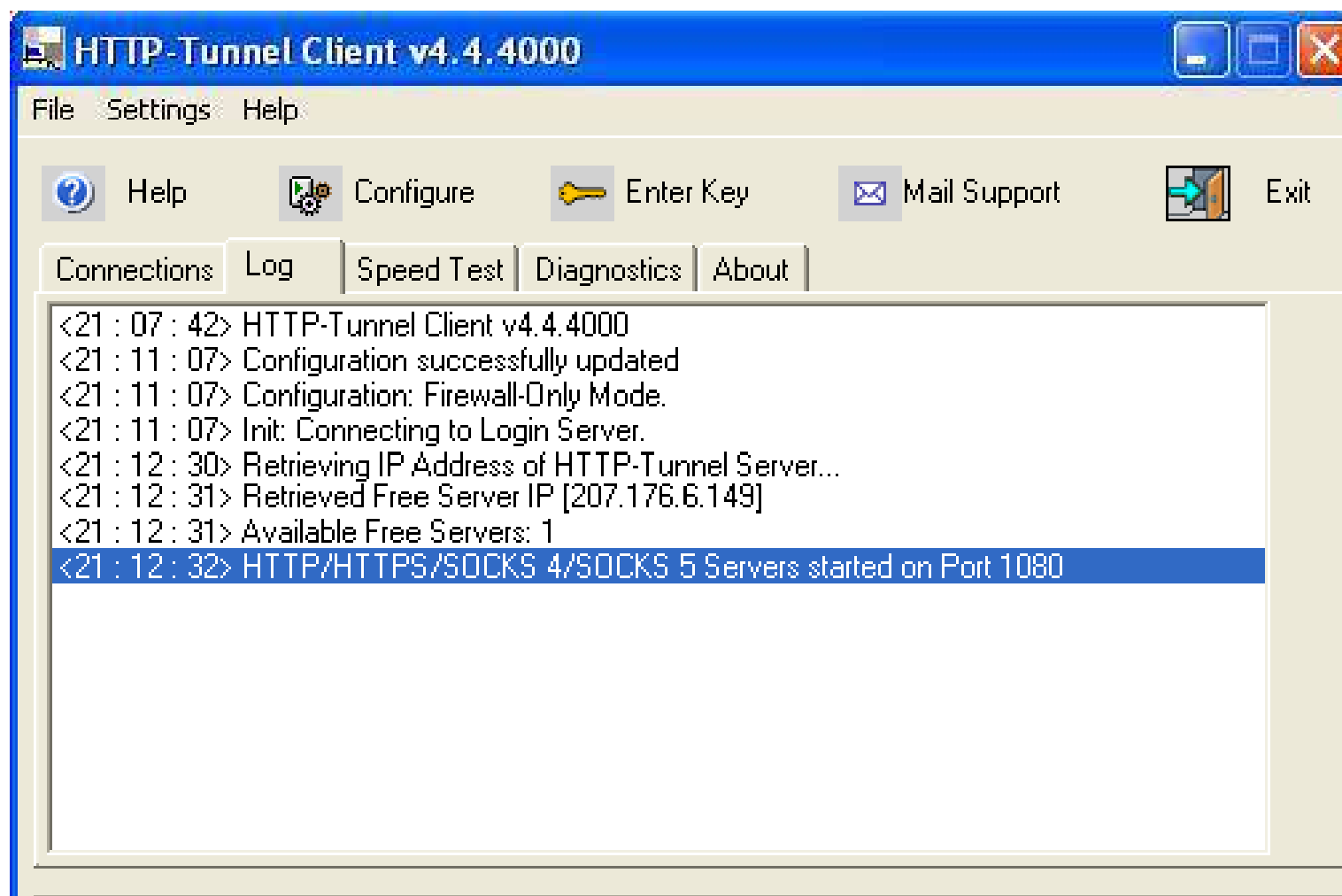
# HTTP-Tunnel: Screenshot 1

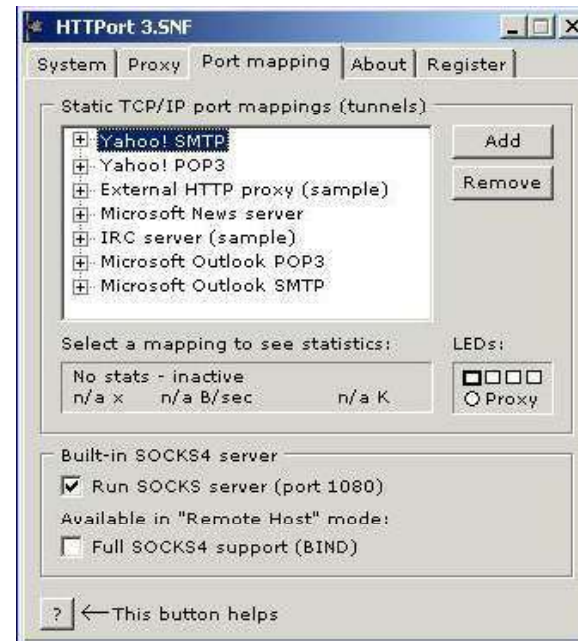


# HTTP-Tunnel: Screenshot 2



# HTTP-Tunnel: Screenshot 3





HTTPort (client) and HTTHost (server) are free tools which can be used to tunnel any TCP traffic through HTTP protocol

Visit <http://www.htthost.com> for more information

It is a free open source tool. Source code is available on the Internet

# Spooftng IP Address

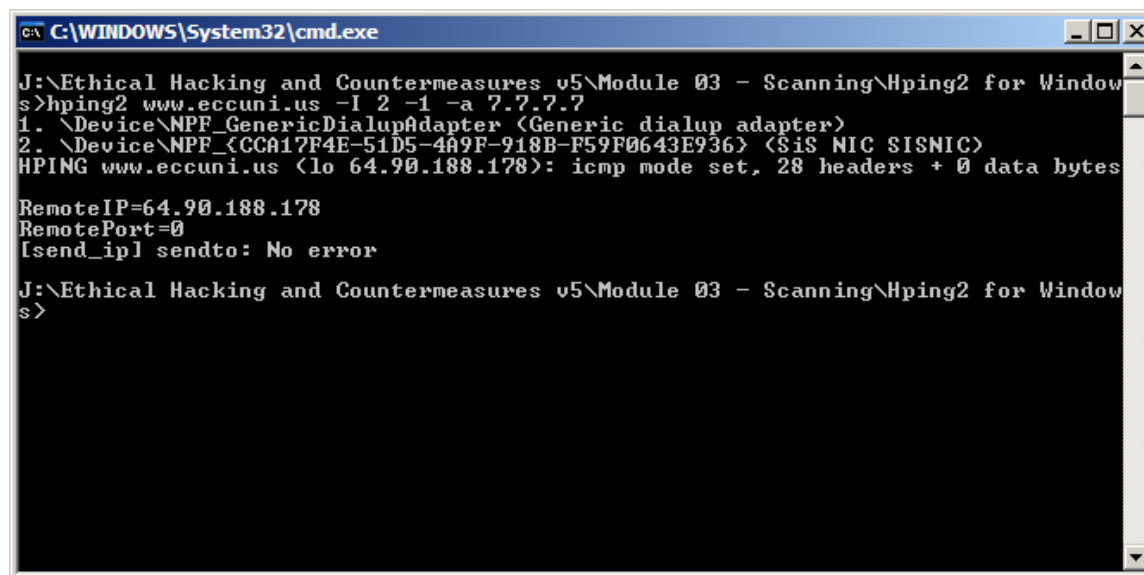
IP Spoofing is when an attacker changes his IP address so that he/ she appears to be someone else

When the victim replies back to the address, it goes back to the spoofed address and not to the attacker's real address

You will not be able to complete the three-way handshake and open a successful TCP connection by spoofing an IP address

Example: (7.7.7.7 is the spoofed address)

```
Hping2 www.eccuni.us -a 7.7.7.7
```



```
C:\WINDOWS\System32\cmd.exe
J:\Ethical Hacking and Countermeasures v5\Module 03 - Scanning\Hping2 for Window
s>hping2 www.eccuni.us -I 2 -l -a 7.7.7.7
1. \Device\NPF_GenericDialupAdapter {Generic dialup adapter}
2. \Device\NPF_{CCA17F4E-51D5-4A9F-918B-F59F0643E936} {SiS NIC SiS NIC}
HPING www.eccuni.us (lo 64.90.188.178): icmp mode set, 28 headers + 0 data bytes

RemoteIP=64.90.188.178
RemotePort=0
[send_ip] sendto: No error

J:\Ethical Hacking and Countermeasures v5\Module 03 - Scanning\Hping2 for Window
s>
```

# Spoofting IP Address



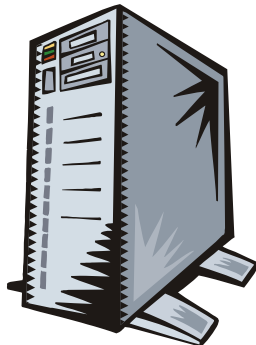
**Attacker**  
10.0.0.5

From Address: 10.0.0.5  
To Address: 10.0.0.25



**Peter**  
10.0.0.25

*Replies sent back to 10.0.0.50*



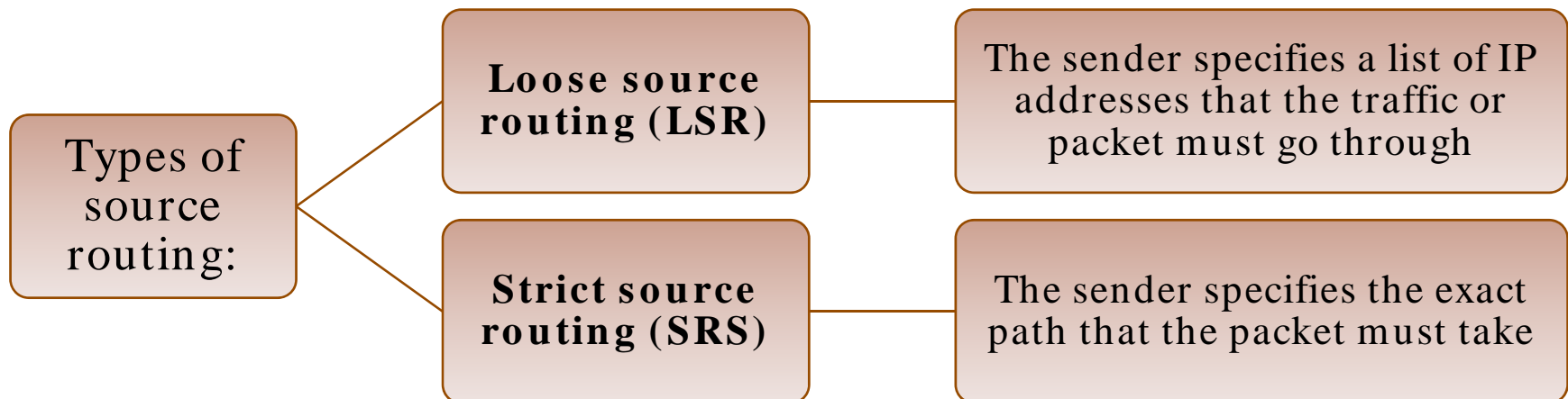
**Spoofted Address**  
10.0.0.50

# Spoofing IP Address Using Source Routing

For this technique to work, an attacker must inject himself into the path that traffic would normally take, to get from the destination machine back to the source

Source routing allows you specify the path a packet will take through the Internet

Source routing feature is built into the TCP/IP protocol suite





# Spoofting IP Address Using Source Routing (cont'd)

Source routing works by using a 39-byte source route option field in the IP header

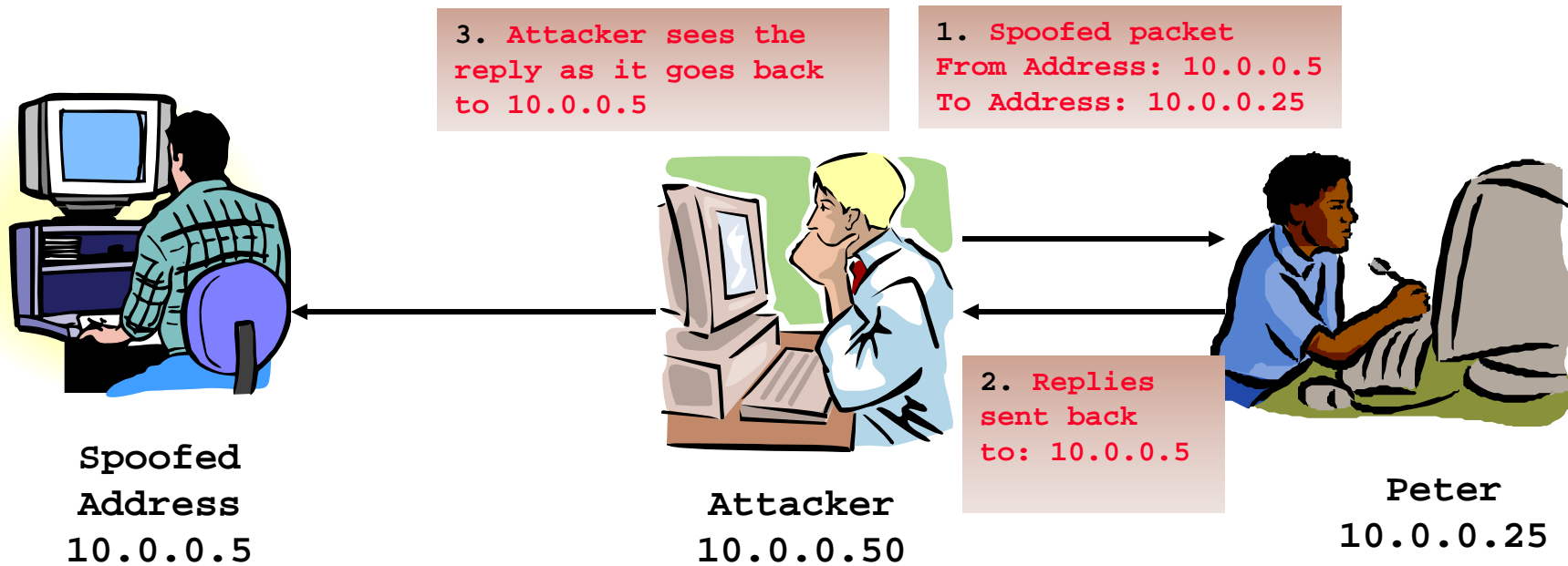
You can specify upto 8 IP addresses in this field

An attacker sends a packet to the destination with a spoofed address but specifies loose source routing and puts his IP address in the list

When the recipient responds, the packet goes to the attacker's machine before reaching the spoofed address

# Spoofing IP Address Using Source Routing (cont'd)

For this technique to work, an attacker must inject himself into the path that traffic would normally take to get from the destination machine back to the source



# Source Routing Command

The command in Windows:

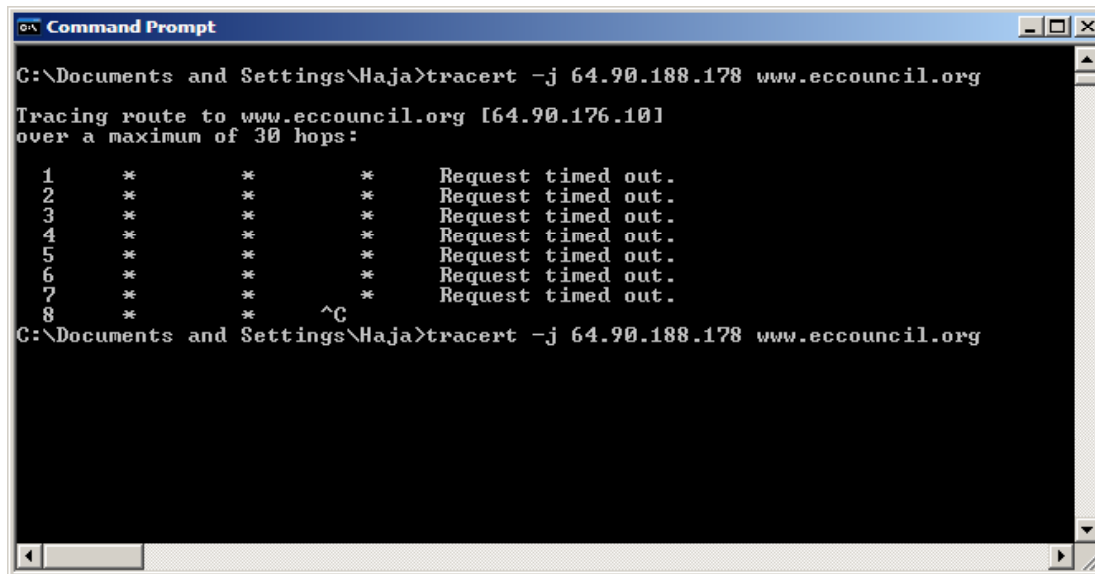
- `tracert -j 10.0.0.50 10.0.0.5`

The command in hping2:

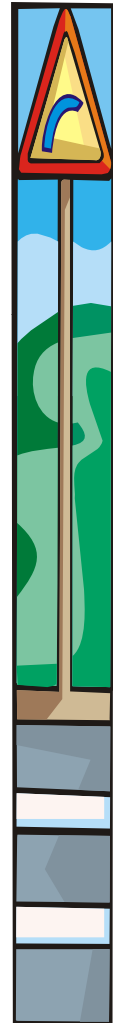
- `hping2 -G 10.0.0.50 10.0.0.5`

Countermeasures

- **DISABLE IP SOURCE ROUTING AT THE ROUTER**



```
Command Prompt
C:\Documents and Settings\Haja>tracert -j 64.90.188.178 www.eccouncil.org
Tracing route to www.eccouncil.org [64.90.176.101]
over a maximum of 30 hops:
  1  *      *      *      Request timed out.
  2  *      *      *      Request timed out.
  3  *      *      *      Request timed out.
  4  *      *      *      Request timed out.
  5  *      *      *      Request timed out.
  6  *      *      *      Request timed out.
  7  *      *      *      Request timed out.
  8  *      *      *      Request timed out.
^C
C:\Documents and Settings\Haja>tracert -j 64.90.188.178 www.eccouncil.org
```



# Detecting IP Spoofing

When an attacker is spoofing packets, he/ she is usually at a different location than the address being spoofed

Attacker's TTL will be different from the spoofed address' real TTL

If you check the received packet's TTL with spoofed one, you will see TTL does not match

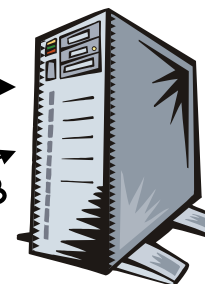


Attacker

Sending a packet with spoofed  
10.0.0.5 IP - TTL 13



Spoofed Address  
10.0.0.5



Target

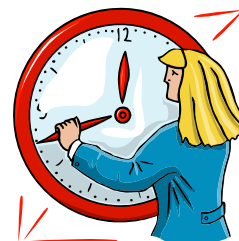
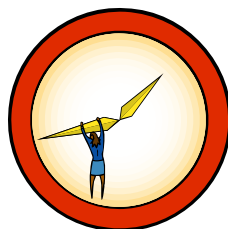
10.0.0.5 IP - TTL 8

# Despoof Tool

Despoof is a free, open source tool that measures the TTL to determine whether or not a packet has been spoofed

The idea is simple - if you receive a packet that you suspect is spoofed, try to determine the real TTL of the packet and compare it to the TTL of the packet you received

```
# ./despoof -h
USAGE:
./despoof [opts] [-d dev] [-i 0-3] [-l(p num )] [-s src] [-t sec] [-T TTL] target
opts are a h v
  -a set ACK flag on TCP packets (does nothing on ICMP)
  -h this help screen
  -v verbose
  -d device to grab local IP or sniff from, default is eth0
  -l local port to bind to, default is 80
  -p target port to send to, default is 80
  -i inquiry packet type to send/receive, types include the following:
      1 tcp (default)
      2 icmp echo
      3 icmp timestamp
  -s spoofed source address
  -t time in seconds to wait for all replies (default 10)
  -T TTL to test (required)
target (IP address or hostname)
```



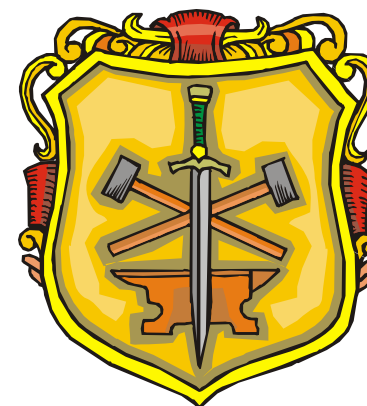
# Scanning Countermeasures

The firewall of a particular network should be good enough to detect the probes of an attacker. The firewall should carry out inspection having a specific rule set

Network intrusion detection systems should be used to find out the OS detection method used by some tools such as Nmap

Only necessary ports should be kept open and the rest should be filtered

All sensitive information that is not to be disclosed to the public over the Internet, should not be displayed



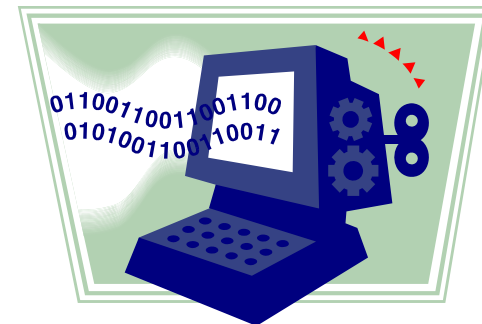
# Tool: SentryPC

Secure Filtering, Monitoring, and Access Control

SentryPC enables you to control, restrict, and monitor access and usage of your PC

## Features:

- Complete Time Management
- Application-on Scheduling and Filtering
- Website Filtering
- Chat Filtering
- Keystroke Filtering
- Powerful Security Features
- Protects your Users
- Logs
  - Keystrokes Typed
  - Application Usage
  - Website Visits
  - Chat Conversations
  - Windows Viewed

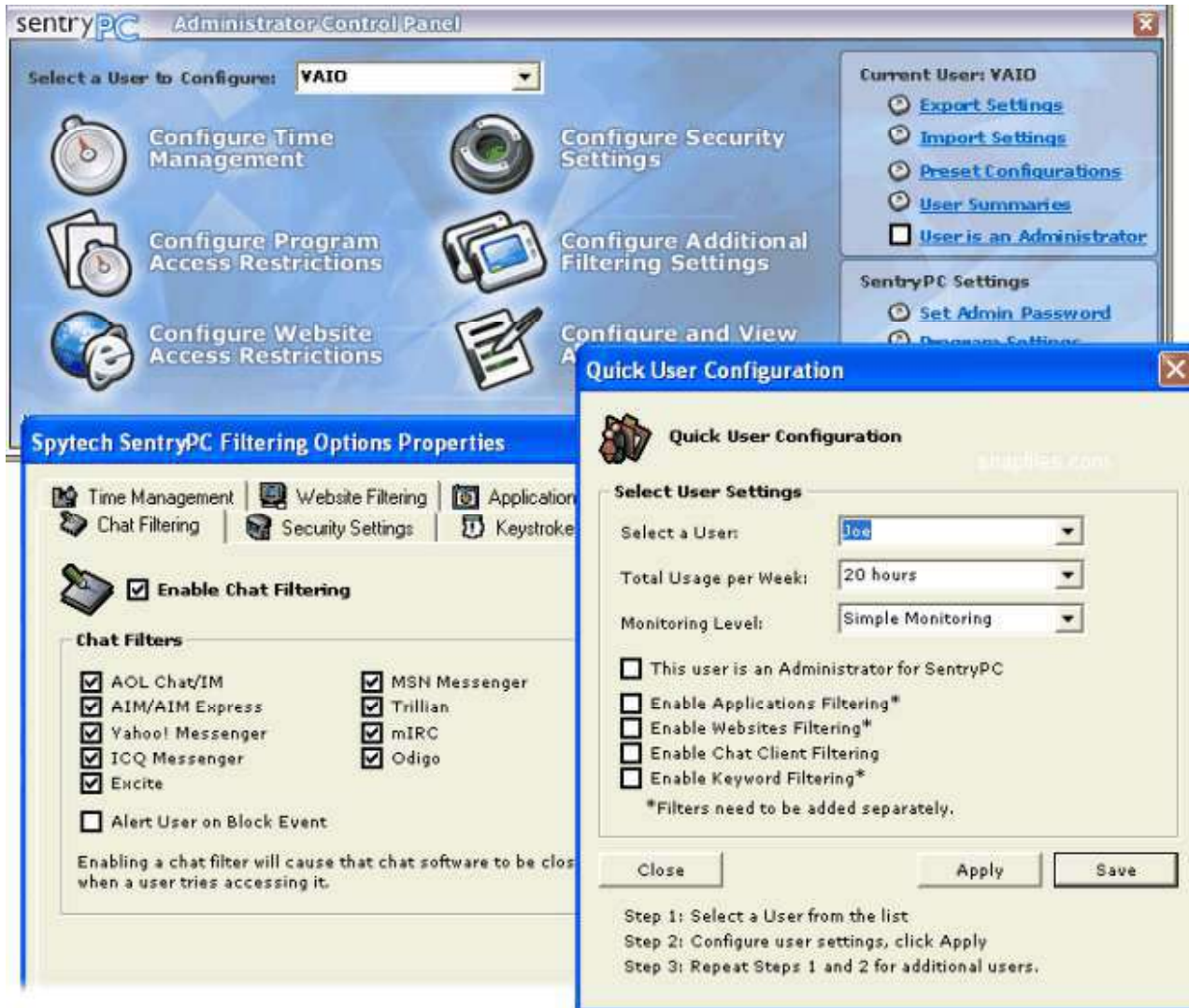




# SentryPC: Screenshot 1



# SentryPC: Screenshot 2



# What Happened Next?

Stephen could not believe the information that was exposed after the scan. Stephen could lay his hands on the following information:

- Operating System of the Web server
- System services
- Firewall mechanism
- Vulnerabilities present on the web server



**ATTACK!!**

# Summary

Scanning is one of the three components of intelligence gathering for an attacker

The objective of scanning is to discover live systems, active/running ports, the operating systems, and the services running on the network

FTP bounce scanning is a type of port scanning which makes use of the Bounce attack vulnerability in FTP servers

War dialing involves the use of a program in conjunction with a modem to penetrate the modem-based systems of an organization by continually dialing in

OS fingerprinting is the method to determine the operating system that is running on the target system

Proxy is a network computer that can serve as an intermediate for connecting with other computers

A chain of proxies can be created to evade the traceback of the attacker

© 1998 Randy Glasbergen. E-mail: randy@glasbergen.com



**“We were way ahead of schedule, so we revised the schedule. Now we’re way behind schedule because we lost too much time revising the schedule. What we need is a schedule to help us revise our schedules on schedule.”**

Copyright 2001 by Randy Glasbergen.  
[www.glasbergen.com](http://www.glasbergen.com)



**“How do they expect us to learn time management when every hour here feels like three hours, a week feels like a year, and the weekends fly by like ten minutes?”**