“Extreme IP Backtracing”

By Lawrence Baldwin & Jaeson Schultz
I've been attacked... now what?

The reality is that few attacks are launched directly from an attacker's system since they know they would be easily caught using standard backtracking methods.

The Internet is chock full of insecure systems which are easily (read already) compromised, providing a means for attackers to perform untraceable, indirect attacks.
The only profound way to improve overall Internet security is to:

- Reduce the total number of compromised hosts
- Minimize the amount of time that any system remains in a compromised state
In order to protect ourselves, we need to ensure that others are protected.

Every time your firewall or intrusion detection system logs an event, don't assume the source is the actual attacker.

Think of it as a cry for help from a likely victim whose system has been compromised and is just being controlled by an attacker.

When we discover that someone is obviously exposed, we should let them know and guide them to the information they need to get protected.
“Authorities pursuing the attackers say the servers they used belonged to users that had no idea their resources were being used to launch attacks.”

*CNN.com article “Avoiding future denial-of-service attacks” about the Feb 2000 DDOS attacks on Yahoo, eBay, Amazon.com and E*Trade*
Why notify victims?

Recently, myNetWatchman detected an incident in which a host was infected with the Microsoft SQL Spida Worm. A backtrace of the offending IP yielded some interesting results...

```
% This is the RIPE Whois server.
% The objects are in RPSL format.
% Please visit http://www.ripe.net/rpsl for more information.
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

inetnum: 194.190.139.0 - 194.190.139.255
netname: GAN
descr: Central Region of GAN RF
country: RU
admin-c: AV753-RIPE
tech-c: AV753-RIPE
status: ASSIGNED PA
notify: sam@gan.ru
notify: ip-reg@ripn.net
mnt-by: ROSNIIROS-MNT
changed: ip-dbм@ripn.net 19991018
source: RIPE
```
"Federal supervision of Russia on nuclear and radiating safety (Gosatomnadzor of Russia) as the federal enforcement authority, organizes and carries out state regulation of safety at use of an atomic energy, nuclear materials, radioactive substances and products on their basis in the peace and defensive purposes (except for regulation of the activity connected to development, manufacturing, test, operation of the nuclear weapon and nuclear power installations of military purpose(assignment))."
The Backtracing Process
Source IP Validation
Confirm the Source of Traffic

- Local Network
- Extended Local Network (e.g. cable modem neighbor)
- Internet
Exclude the ‘Martian Addresses’

- Broadcast: 0.0.0.0/8
- Loopback: 127.0.0.0/8
- Multicast: 224.0.0.0/4
- Limited Broadcast: 255.255.255.255/32

“A router SHOULD NOT forward any packet that has an invalid IP source address”

RFC1812 - Requirements for IP Version 4 Routers – Section 5.3.7
Martian Address Filtering
"The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets:

- 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)"

RFC1918 - Address Allocation for Private Internets
**Solution to the Korean Spam problem?**

<table>
<thead>
<tr>
<th>ENGLISH</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Address</strong> : 172.21.3.168-172.21.3.199</td>
</tr>
<tr>
<td><strong>Connect ISP Name</strong> : DREAMX</td>
</tr>
<tr>
<td><strong>Connect Date</strong> : 20000622</td>
</tr>
<tr>
<td><strong>Registration Date</strong> : 20000706</td>
</tr>
<tr>
<td><strong>Network Name</strong> : DSB</td>
</tr>
<tr>
<td><strong>Organization Information</strong></td>
</tr>
<tr>
<td><strong>Orgnization ID</strong> : ORG127773</td>
</tr>
<tr>
<td><strong>Name</strong> : DSB</td>
</tr>
<tr>
<td><strong>State</strong> : PUSAN</td>
</tr>
<tr>
<td><strong>Address</strong> : Billra Dangrishinik 407 Dangri-Dong</td>
</tr>
<tr>
<td><strong>Zip Code</strong> : 604-010</td>
</tr>
<tr>
<td><strong>Admin Contact Information</strong></td>
</tr>
<tr>
<td><strong>Name</strong> : YOUNGKIL SHIN</td>
</tr>
<tr>
<td><strong>Org Name</strong> : DREAMX</td>
</tr>
<tr>
<td><strong>State</strong> : SEOUL</td>
</tr>
<tr>
<td><strong>Address</strong> : 12F World Tower 7-25 Shincheon-Dong Songpa-Gu</td>
</tr>
<tr>
<td><strong>Zip Code</strong> : 138-240</td>
</tr>
<tr>
<td><strong>Phone</strong> : +82-2-3434-1790</td>
</tr>
<tr>
<td><strong>Fax</strong> : +82-2-3434-1799</td>
</tr>
<tr>
<td><strong>E-Mail</strong> : <a href="mailto:ykshin@cjdream.net">ykshin@cjdream.net</a></td>
</tr>
<tr>
<td><strong>Technical Contact Information</strong></td>
</tr>
<tr>
<td><strong>Name</strong> : SUKBONG KIM</td>
</tr>
<tr>
<td><strong>Org Name</strong> : DREAMX</td>
</tr>
<tr>
<td><strong>State</strong> : SEOUL</td>
</tr>
<tr>
<td><strong>Address</strong> : 12F World Tower 7-25 Shincheon-Dong Songpa-Gu</td>
</tr>
<tr>
<td><strong>Zip Code</strong> : 138-240</td>
</tr>
<tr>
<td><strong>Phone</strong> : +82-2-3434-1768</td>
</tr>
<tr>
<td><strong>Fax</strong> : +82-2-3434-1799</td>
</tr>
<tr>
<td><strong>E-Mail</strong> : <a href="mailto:sbkim091@dreamx.net">sbkim091@dreamx.net</a></td>
</tr>
</tbody>
</table>
### Exclude IANA Addresses*

<table>
<thead>
<tr>
<th>Address</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESERVED-9</td>
<td>1.0.0.0 - 1.255.255.255</td>
</tr>
<tr>
<td>RESERVED-2</td>
<td>2.0.0.0 - 2.255.255.255</td>
</tr>
<tr>
<td>PDN</td>
<td>14.0.0.0 - 14.255.255.255</td>
</tr>
<tr>
<td>RESERVED-23</td>
<td>23.0.0.0 - 23.255.255.255</td>
</tr>
<tr>
<td>RESERVED-31</td>
<td>31.0.0.0 - 31.255.255.255</td>
</tr>
<tr>
<td>RESERVED-37</td>
<td>37.0.0.0 - 37.255.255.255</td>
</tr>
<tr>
<td>RESERVED-39A</td>
<td>39.0.0.0 - 39.255.255.255</td>
</tr>
<tr>
<td>RESERVED-41A</td>
<td>41.0.0.0 - 41.255.255.255</td>
</tr>
<tr>
<td>RESERVED-58</td>
<td>58.0.0.0 - 58.255.255.255</td>
</tr>
<tr>
<td>RESERVED-59</td>
<td>59.0.0.0 - 59.255.255.255</td>
</tr>
<tr>
<td>RESERVED-60</td>
<td>60.0.0.0 - 60.255.255.255</td>
</tr>
<tr>
<td>RESERVED-7</td>
<td>69.0.0.0 - 79.255.255.255</td>
</tr>
<tr>
<td>RESERVED-11</td>
<td>82.0.0.0 - 95.255.255.255</td>
</tr>
<tr>
<td>RESERVED-8</td>
<td>96.0.0.0 - 126.255.255.255</td>
</tr>
</tbody>
</table>

*Note: This information is subject to change. Looking up ‘IANA’ at ARIN.net will give you the current list.*
<table>
<thead>
<tr>
<th>Prefix</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESERVED-3</td>
<td>128.0.0.0 - 128.0.255.255</td>
</tr>
<tr>
<td>BLACKHOLE.ISI.EDU</td>
<td>128.9.64.26</td>
</tr>
<tr>
<td>TEST-B</td>
<td>128.66.0.0 - 128.66.255.255</td>
</tr>
<tr>
<td>LINKLOCAL</td>
<td>169.254.0.0 - 169.254.255.255</td>
</tr>
<tr>
<td>RESERVED</td>
<td>191.255.0.0 - 191.255.255.255</td>
</tr>
<tr>
<td>RESERVED-192</td>
<td>192.0.0.0 - 192.0.127.255</td>
</tr>
<tr>
<td>ROOT-NS-LAB</td>
<td>192.0.0.0 - 192.0.0.255</td>
</tr>
<tr>
<td>NET-ROOTS-NS-LIVE</td>
<td>192.0.1.0 - 192.0.1.255</td>
</tr>
<tr>
<td>NET-TEST</td>
<td>192.0.2.0 - 192.0.2.255</td>
</tr>
<tr>
<td>RESERVED-2A</td>
<td>192.0.128.0 - 192.0.255.255</td>
</tr>
<tr>
<td>RESERVED-2-A</td>
<td>192.0.128.0 - 192.0.255.255</td>
</tr>
<tr>
<td>IANA-192</td>
<td>192.88.99.0 - 192.88.99.255</td>
</tr>
<tr>
<td>RESERVED-13</td>
<td>197.0.0.0 - 197.255.255.255</td>
</tr>
<tr>
<td>RESERVED-14</td>
<td>201.0.0.0 - 201.255.255.255</td>
</tr>
<tr>
<td>RESERVED</td>
<td>221.0.0.0 - 223.255.255.255</td>
</tr>
</tbody>
</table>
Note possibly contrived bogus IPs

improbable octet sequences
• 1.2.3.4
• 5.6.7.8

nmap decoy addresses
• 24.24.24.24
• 23.23.23.23
"The weakness in this scheme [the Internet Protocol] is that the source host itself fills in the IP source host id, and there is no provision in ... TCP to discover the true origin of the packet."

Robert T. Morris writing about IP in his 1985 paper “A Weakness in the 4.2BSD Unix† TCP/IP Software”
Traceroute Hop Count

Step 1: Calculate the *implied* hop count from the packet you received. The *implied* hop count is:

**Original packet TTL - Final TTL** (where you received it)
(Note that you must guess what the original TTL value is.)

Step 2: Traceroute to the IP and get an *actual* hop count. If substantially different from the implied count, then the IP may be spoofed.
### Default TTL Values

<table>
<thead>
<tr>
<th>OS Version</th>
<th>tcp_ttl</th>
<th>udp_ttl</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIX</td>
<td>60</td>
<td>30</td>
</tr>
<tr>
<td>FreeBSD 2.1R</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>HP/UX 9.0x</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td>HP/UX10.01</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>Irix 5.3</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>Irix 6.x</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>Linux</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>MacOS/MacTCP 2.0.x</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>OS/2 TCP/IP 3.0</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>OSF/1 V3.2A</td>
<td>60</td>
<td>30</td>
</tr>
<tr>
<td>Solaris 2.x</td>
<td>255</td>
<td>255</td>
</tr>
<tr>
<td>SunOS 4.1.3/4.1.4</td>
<td>60</td>
<td>60</td>
</tr>
<tr>
<td>MS Windows 95</td>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td>MS Windows NT 3.51</td>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td>MS Windows NT 4.0</td>
<td>128</td>
<td>128</td>
</tr>
</tbody>
</table>

**Source IP Validation**

**Spoof Detection**
Traceroute Hop Count Difficulties

Type escape sequence to abort.
Tracing the route to forthelife.net (216.144.196.7)

1 63.237.160.113 8 msec 12 msec 8 msec
2 lax-core-01.inet.qwest.net (205.171.19.149) 8 msec 8 msec 8 msec
3 sjo-core-03.inet.qwest.net (205.171.5.155) 16 msec 16 msec 16 msec
4 sjo-core-01.inet.qwest.net (205.171.22.10) 16 msec 16 msec 16 msec
5 sfo-core-02.inet.qwest.net (205.171.5.131) 20 msec 48 msec 16 msec
6 chi-core-01.inet.qwest.net (205.171.5.42) 72 msec 64 msec 68 msec
7 chi-core-03.inet.qwest.net (205.171.20.174) 64 msec 64 msec 76 msec
8 chi-edge-17.inet.qwest.net (205.171.20.154) 64 msec 64 msec 68 msec
9 63.149.1.70 80 msec 84 msec 84 msec
10 10.60.1.9 80 msec * 80 msec
11 172.16.250.1 96 msec 84 msec 88 msec
12 * * *
13 * * *
Perform Route Validation

A Looking Glass site allows you to access the routing table on a core router. Using this you can determine if any routes exist to the IP address you are interested in.

http://lg.above.net/
http://nitrous.digex.net/cgi-bin/looking_glass.pl
http://www.merit.edu/~ipma/tools/lookingglass.html
Spoof Example

No match for "182.1.1.2".

%%%%%%%%%%%%%%%%%%%%%%%%% NO MATCH TIP %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%                                                                           %
%  ALL OF THE POINT OF CONTACT HANDLES IN THE ARIN                         %
%  WHOIS END WITH "-ARIN", IF YOU ARE QUERYING A POINT                     %
%  OF CONTACT HANDLE PLEASE ADD -ARIN TO YOUR QUERY.                      %
%                                                                           %
%%%%%%%%%%%%%%%%%%%%%%%%% NO MATCH TIP %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

The ARIN Registration Services Host contains ONLY Internet Network Information: Networks, ASN's, and related POC's. Please use the whois server at rs.internic.net for DOMAIN related Information and whois.nic.mil for NIPRNET Information.
Source IP Validation
Spoof Example contd...

MAE-West Looking Glass Results

Query: bgp
Addr: 182.1.1.2

% Network not in table
Nslookup

Performing a reverse DNS lookup with nslookup can sometimes yield the domain name of the IP address in question. Armed with that domain name, we can query for the domain’s Start of Authority (SOA) contact information.
Nslookup Example

D:\>nslookup
> set type=ptr
> 26.22.209.24.in-addr.arpa
Server:  huey.cbeyond.net
Address:  64.213.152.18

Non-authoritative answer:
26.22.209.24.in-addr.arpa
name = dhcp024-209-022-026.cinci.rr.com

> set type=soa
> 26.22.209.24.in-addr.arpa
Server:  huey.cbeyond.net
Address:  64.213.152.18

*** No start of authority (SOA) records available for
26.22.209.24.in-addr.arpa
Nslookup Example contd...

> 22.209.24.in-addr.arpa
Server: huey.cbeyond.net
Address: 64.213.152.18

Non-authoritative answer:
22.209.24.in-addr.arpa

  primary name server = ns1.columbus.rr.com
  responsible mail addr = noc.columbus.rr.com
  serial = 2000120401
  refresh = 3600 (1 hour)
  retry = 900 (15 mins)
  expire = 604800 (7 days)
  default TTL = 3880 (1 hour 4 mins 40 secs)
whois (IP)

If a reverse DNS query on the IP address fails to turn up any results, the next place to look is in the ARIN whois registry. This can be accessed via HTTP, a whois client, or raw, via port 43.

- If the domain portion of the whois email contact seems to be associated with the organization owning the netblock, then take that as the responsible domain

- Do NOT use the contact mailbox for security issues unless it is a very small netblock (class C or less)
ARIN Whois Query Syntax

To find only a certain **TYPE** of record, use keyword:
- **HOst**
- **ASn**
- **PErson**
- **ORganization**
- **NEtwork**
- **GRoup**

To search only a specific **FIELD**, use keyword or character:
- **HAndle** or "!"
- **Mailbox** or contains "@"
- **NAme** or leading "."

Here are some additional Whois keywords:
- **EXPand** or "*"
  Shows all parts of display without asking
- **Full** or "=
  Shows detailed display for EACH match
- **Help**
  Enters the help program for full documentation
- **PArtial** or trailing "." 
  Matches targets STARTING with the given string
- **Q, QUIT, or Return**
  Exits Whois
- **SUBdisplay** or "%"
  Shows users of host, hosts on net, etc.
- **SUMmary** or "$
  Always shows summary, even if just one match
Internet America (NETBLK-IADFW-BLK3)
350 N St. Paul Suite 200
Dallas TX 75201
US

Netname: IADFW-BLK3
Netblock: 207.136.0.0 - 207.136.63.255
Maintainer: IAM

Coordinator:
Wommack, Mike (MW781-ARIN) m_wommack@hotmail.com
123-456-7890 (FAX) 123-456-7890

Domain System inverse mapping provided by:
NS1.IADFW.NET 206.66.12.36
NS2.IADFW.NET 204.178.72.30

Record last updated on 27-Dec-1996.
Database last updated on 19-Jun-2001 23:00:59 EDT.
Intermediate Backtrace
Recursive whois (IP)

Records that are not administered by ARIN are likely to be found at one of the other regional registries, RIPE and APNIC. Sometimes a query to ARIN will refer you to APNIC who, in turn, will direct you to JPNIC, KRNIC, or one of the national registries.
whois (domain)

Cross-check the domain info returned from a IP based whois query with the domain whois records. Geektools runs a nice proxy that can be used for both IP and domain name queries.
"Under current administrative practices, the usTLD not only has no central database that can in turn create a central Whois, there is also no mechanism in place for delegees to provision database information to the central registry. Even if delegees wished to provide new Whois information to the usTLD administrator, that capability is currently nonexistent."

"NeuStar Response to SB1335-01-Q-0740" Part of NeuStar’s proposal for managing the .us TLD
Mailbox validation

You can use nslookup to get the mail server for a domain, and then manually you can VRFY addresses at the domain. If verification is turned off, you may want to check http://whois.abuse.net

Look up an address in the abuse.net contact database

Database updated July 5, 2002 18:15, current size 107666 entries.

Enter the name of the domain that you would like to check, such as example.com.
Advanced Backtrace
If a whois query doesn’t give you the appropriate domain, try a Google search on organization name adding *parts* of the address info.
Double Netblocks?

Search results for: 205.235.9.204

I-Wave Corp. (NETBLK-NET-IWAVE-HUB) NET-IWAVE-HUB 205.235.0.0 - 205.235.15.255
Cyberholdings Incorporated (NETBLK-CYBERHOLDINGS) CYBERHOLDINGS 205.235.0.0 - 205.235.15.255
Advanced Backtrace
Double Netblocks? contd...

I-Wave Corp. (NETBLK-NET-IWAVE-HUB)
  800 Towers Crescent Dr, ste 1350
  Vienna, VA  22182
  US

Netname: NET-IWAVE-HUB
Netblock: 205.235.0.0 - 205.235.15.255
Maintainer: WAVE

Coordinator:
  Rosenbaum, Alex (AR143-ARIN) alexrosenbaum@hotmail.com
  (240) 462-8655

Domain System inverse mapping provided by:

DNS1.HOY.NET 205.235.2.130
NS2.CW.NET 204.70.57.242
Database last updated on 21-Mar-2002 19:58:27 EDT.
Double Netblocks? contd...

Advanced Backtrace

ebizQ.net: The Portal for e-Business Integration
... Understanding Enterprise Messaging and Standards-Based Integration:
A Technical Seminar by Sonic Software, 2002-06-13, Vienna, VA ...
www.ebizq.net/ - 43k - Cached - Similar pages

Message Q - News
... News Search by Category ...
www.ebizq.net/news/ - 45k - Cached - Similar pages

Netplex Internet Access Providers
... iWave address: 6800 Tower Crescent Dr., Suite 1350, Vienna, VA 22182: Web site:
http://www.iwave.com; email: auto-responder: info@iwave.com; voice: (703) 760 ...
www.ens.com/serv/Netplexacc.html - 26k - Cached - Similar pages

Newsletter 2000-03
... and have not received a confirmation e-mail, please send e-mail to iwave ... YTEC2000
Organization Committee KSEA, 1952 Gallows Road, Suite 300, Vienna, VA ...
www.public.asu.edu/~smiee/KASA/newsletter/0003.html - 14k - Cached - Similar pages

Message Q - News
Advanced Backtrace
Double Netblocks? contd…
“RWhois (Referral Whois) extends and enhances the Whois concept in a hierarchical and scaleable fashion. In accordance with this, RWhois focuses primarily on the distribution of "network objects", or the data representing Internet resources or people, and uses the inherently hierarchical nature of these network objects (domain names, Internet Protocol (IP) networks, email addresses) to more accurately discover the requested information.”

RFC2167 - Referral Whois (RWhois) Protocol V1.5
Rwhois server data:

```
$ rwhois V-1.5:001ab7:00 rwhois.exodus.net (Exodus Communications)
network:Class-Name:network
network:Auth-Area:0.0.0.0/0
network:Network-Name:216.34.168.128
network:IP-Network:216.34.168.128/26
network:Organization:I:Pixel Magic Imaging
network:Name:I:Alfred Grant Lewis
network:Email:I:glewis@pixelimaging.com
network:Street:I:531 Mill Street
network:City:I:San Marcos
network:State:I:TX
network:Postal-Code:I:78666
network:Country-Code:I:USA

network:Class-Name:network
network:Auth-Area:0.0.0.0/0
network:Network-Name:216.34.160.0
network:IP-Network:216.34.160.0/20
network:Organization:I:Exodus IDC - AU/AU
network:Name:I:Exodus IP Address Administrator
network:Email:I:ipaddressadmin@exodus.net
network:Street:I:1418 Park Center Drive Building 1
network:City:I:Austin
network:State:I:TX
network:Postal-Code:I:78753
network:Country-Code:I:USA

network:Class-Name:network
network:Auth-Area:0.0.0.0/0
network:Network-Name:216.32.0.0
network:IP-Network:216.32.0.0/14
network:Organization:I:Exodus Communications (Exodus Legacy)
network:Name:I:Exodus Hostmaster
network:Phone:I:800-6233-9787
network:Email:I:ipaddressadmin@exodus.net
network:Street:I:2831 Mission College Boulevard
network:City:I:Santa Clara
```

Registrant:
David Oles (PMIMAGING2-DOM)
   631 Mill Street
   San Marcos, TX 78666
   US

Domain Name: PMIMAGING.COM

Administrative Contact, Technical Contact:
Melancon, Mark (ILLYVXOEGO)hostmaster@PMIMAGING.COM
Pixel Magic Imagin/IT Manager
631 Mill Street
San Marcos, TX 78666
US
512 396 7251
Fax- 512 396 8767
Routing Registry (RR Records)

Internet routing registries, as described in the Routing Policy Specification Language, RPSL (RFC2280) document, provides a view of the global routing policy to improve the integrity of the Internet's routing.
Success with RR

Click Network/Local Access (NETBLK-GBX-REQ000000014080)
1111 Altheimer Street South
Tacoma, WA 98402
US

Netname: GBX-REQ000000014080
Netblock: 208.51.248.0 - 208.51.251.255

Coordinator:
Global Crossing (IA12-ORG-ARIN) ipadmin@gblx.net
+1 800 404-7714

Record last updated on 29-Nov-2001.
Database last updated on 28-Apr-2002 19:58:33 EDT.

The ARIN Registration Services Host contains ONLY Internet Network Information: Networks, ASN's, and related POC's. Please use the whois server at rs.internic.net for DOMAIN related Information and whois.nic.mil for NIPRNET Information.
% ARIN Internet Routing Registry Whois Interface

route:      208.51.251.0/24
descr:      Customer Local Access
origin:     AS20394
notify:     hostmaster@click-network.com
mnt-by:     MAINT-AS14677
changed:    sroberts@click-network.com 20020110
source:     RADB

route:      208.48.0.0/14
descr:      GBLX-US-AGGREGATE
origin:     AS3549
mnt-by:     GBLX-RIPE-MNT
changed:    dcooper@globalcenter.net 19991229
source:     RIPE
Extreme Backtrace
Mail Banner?

Telnet to port 25 and see if the IP address runs a mailserver and has possibly published a useful banner. Other well known ports may be tried as well (POP, FTP, etc.)
Extreme Backtrace

Contact information gleaned from SSL Cert.

Certificate

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>V3</td>
</tr>
<tr>
<td>Serial number</td>
<td>24D6 E145 A46D 05DC 0909 3...</td>
</tr>
<tr>
<td>Signature algorithm</td>
<td>md5RSA</td>
</tr>
<tr>
<td>Issuer</td>
<td><a href="http://www.verisign.com/CPS">www.verisign.com/CPS</a> Incorp...</td>
</tr>
<tr>
<td>Valid From</td>
<td>Wednesday, July 11, 2001 8:...</td>
</tr>
<tr>
<td>Valid to</td>
<td>Friday, July 12, 2002 7:59:59...</td>
</tr>
<tr>
<td>Subject</td>
<td><a href="http://www.latimes.com">www.latimes.com</a>, Tribune Int...</td>
</tr>
<tr>
<td>Public key</td>
<td>RSA (1024 bits)</td>
</tr>
</tbody>
</table>

CN = www.latimes.com
OU = Tribune Interactive
O = Tribune Company
L = Chicago
S = Illinois
C = US
**Gone too far?**

% This is the RIPE Whois server.  
% The objects are in RPSL format.  
% Please visit http://www.ripe.net/rpsl for more information.  
% Rights restricted by copyright.  
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

netname: EMSERTEX  
descr: Red de EMSERTEX  
descr: Spain  
country: ES  
admin-c: EDMO-RIPE  
tech-c: REPR-RIPE  
status: ASSIGNED PA  
mnt-by: UNI2-MNT  
changed: emorenoz@uni2.es 20020419  
source: RIPE

route: 62.36.0.0/16  
descr: Uni2 PA Block 1  
origin: AS12479  
mnt-by: UNI2-MNT  
changed: natalayero@uni2.es 19990806
ftp> open 62.36.225.185
Connected to 62.36.225.185.

220 m3hdesmertex FTP server (Version wu-2.6.0(1)
User (62.36.225.185:(none)):
Extreme Backtrace
Gone too far? contd...
Registrant:
Acosta Gestion S.L.
C/Severo Ochoa
Madrid, Madrid 28230
ES

Domain Name: PORTALADULTOS.COM

Administrative Contact, Technical Contact, Zone Contact:
Acosta Gestion S.L.
Esteban Acosta
Calle Dr. Madrid 1
Madrid, Madrid 28220
ES
011916340101
webmaster@portaladultos.com

Domain created on 21-May-2001
Domain expires on 21-May-2003
Last updated on 29-Apr-2002

Domain servers in listed order:
DNS.COMTENIDOS.COM           62.37.225.56
DNS2.COMTENIDOS.COM          62.37.225.57
Still no answer?
Identify responsible AS

Lookup IP in BGP route tables to identify which Autonomous System is responsible for the route. Then, identify the responsible domain by doing recursive Whois AS lookups.
The Quality of AS data

MAE-East Looking Glass Results

```
Query: bgp
Addr: 205.152.0.20

BGP routing table entry for 205.152.0.0/20, version 27329530

Paths: (3 available, best #2)
  Advertised to peer-groups:
    tt-pop
      7.8.1.6197
    165.117.68.190 (metric 105100) from 165.117.1.160 (165.117.1.147)
      Origin IGP, metric 6, localpref 100, valid, internal
      Community: 2548:180 2548:254 2548:666 3706:102
      Originator: 165.117.1.147, Cluster list: 165.117.1.160, 165.117.161.7, 165.117.162.202, 165.117.68.190
    701 6197
    165.117.68.190 (metric 105100) from 165.117.1.52 (165.117.1.147)
      Origin IGP, metric 6, localpref 100, valid, internal, best
      Community: 2548:180 2548:254 2548:666 3706:102
      Originator: 165.117.1.147, Cluster list: 165.117.1.52, 165.117.162.200, 165.117.162.202, 165.1
    701 6197
    165.117.68.190 (metric 105100) from 165.117.1.147 (165.117.1.147)
      Origin IGP, metric 4294967294, localpref 100, valid, internal
      Community: 2548:180 2548:254 2548:666 3706:102
```
### Output from ARIN Whois

<table>
<thead>
<tr>
<th>ARIN Home Page</th>
<th>ARIN Site Map</th>
<th>ARIN Whois Help</th>
<th>NEW! Database &amp; Template Conversion Information Center</th>
</tr>
</thead>
</table>

Search for: [Input Field] [Submit]

#### Search results for: AS 6197

BellSouth Network Solutions, Inc (ASN-BATI-ATL)
1100 Ashwood Parkway, Suite 200
Atlanta, Ga. 30338
US

Autonomous System Name: BATI-ATL
Autonomous System Number: 6197

Coordinator:
Dawson, Willard (WD14-ARIN) willard.dawson@SBS.SIEMENS.COM
770 814 5099 (FAX) 770 814 5280

Record last updated on 04-Jan-1996.
Database last updated on 8-Jul-2002 20:01:39 EDT.
### Advanced Backtrace
The Quality of AS data contd...

#### Output from ARIN Whois

<table>
<thead>
<tr>
<th>ARIN Home Page</th>
<th>ARIN Site Map</th>
<th>ARIN Whois Help</th>
<th>NEW! Database &amp; Template Conversion Information Center</th>
</tr>
</thead>
</table>

**Search results for: WD14-ARIN**

Dawson, Willard (WD14-ARIN)  
Siemens Business Services  
Siemens Business Services  
4570 River Green Parkway, Suite 140  
Duluth, GA 30096-2564  
770 814 5099 (FAX) 770 814 5280

willard.dawson@SBS.SIEMENS.COM

Record last updated on 13-Nov-1997.  
Database last updated on 8-Jul-2002 20:01:39 EDT.
Netbios enabled?

See if IP has Netbios enabled and can receive a Winpopup message

Example (From DOS)
C: \> nbtstat -A 24.24.24.24

If you get a response, then:
C: \> net send 24.24.24.24 "FYI, You've been hacked, .... instructions ..."

Still no answer?
Netbios Backtrace

D:\gdtest>nbtstat -A 208.254.151.185

Local Area Connection:
Node IpAddress: [172.16.1.169] Scope Id: []

NetBIOS Remote Machine Name Table

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>HLM</td>
<td>&lt;00&gt;</td>
<td>UNIQUE</td>
</tr>
<tr>
<td>ADDUCCI_DORF</td>
<td>&lt;00&gt;</td>
<td>GROUP</td>
</tr>
<tr>
<td>HLM</td>
<td>&lt;03&gt;</td>
<td>UNIQUE</td>
</tr>
<tr>
<td>HLM</td>
<td>&lt;20&gt;</td>
<td>UNIQUE</td>
</tr>
<tr>
<td>ADDUCCI_DORF</td>
<td>&lt;1E&gt;</td>
<td>GROUP</td>
</tr>
</tbody>
</table>

MAC Address = 00-50-8B-6A-32-63

Still no answer?
D:\>tracert 208.254.151.185

Tracing route to HLM [208.254.151.185]
over a maximum of 30 hops:

1  10 ms  <10 ms  <10 ms  host121.mynetwatchman.com [64.238.113.121]
2  <10 ms  <10 ms  10 ms  172.16.41.165
3  <10 ms  10 ms  <10 ms  car00-s6-0-1.atlagabu.cbeyond.net [192.168.14.17]
4  <10 ms  10 ms  <10 ms  bgr00-g2-0.atlagabu.cbeyond.net [192.168.18.49]
5  <10 ms  10 ms  10 ms  s1-0-0.arl1.ATL1.gblx.net [64.211.166.201]
6  <10 ms  10 ms  10 ms  pos2-0-155M.crl1.ATL1.gblx.net [206.132.115.113]
7  <10 ms  10 ms  10 ms  pos0-0-0-155M.br1.ATL1.gblx.net [206.132.115.118]
8  <10 ms  10 ms  10 ms  57.ATM2-0.BR1.ATL5.ALTER.NET [204.255.168.137]
9  <10 ms  10 ms  10 ms  0.so-2-3-0.XL2.ATL5.ALTER.NET [152.63.82.194]
10 <10 ms  10 ms  10 ms  0.so-1-2-0.TL2.ATL5.ALTER.NET [152.63.146.2]
11 40 ms  31 ms  40 ms  0.so-6-0-2.TL2.CH14.ALTER.NET [152.63.13.45]
12 40 ms  40 ms  40 ms  0.so-0-0-0.XL2.CH14.ALTER.NET [152.63.13.33]
13 30 ms  40 ms  40 ms  0.so-4-0-0.XR2.CH14.ALTER.NET [152.63.2.58]
14 40 ms  40 ms  40 ms  194.ATM7-0.GW4.CH1.ALTER.NET [152.63.68.229]
15 50 ms  40 ms  50 ms  HLM [208.254.151.185]

Trace complete.

Still no answer?
Netbios Backtrace Contd...
Netbios Backtrace Contd...

Still no answer?

2 "Astronomical Figures," University of Chicago Magazine, ...
... Dorf, a partner in the general-practice law firm Adducci, Dorf, Lehner, Mitchell & Blankenship, PC, in Chicago, is writing a musical based on Yerkes' life. ...
www2.uchicago.edu/alumni/alumni.mag/9702/5702Yeikes6.html - 6k - Cached - Similar pages

"D" Chicago Lawyers
... 312/565-0832. Michael C. Dorf Adducci Dorf et al Sto 2130 150 N.
Michigan Ave. Chicago IL 60601 312/781-2806 312/781-2611. Karen M ...
www.lawhost.com/chicagolist/ChiLawyers-D.html - 25k - Cached - Similar pages

SYMPOSIUM PROCEEDINGS
File Format: PDF/Adobe Acrobat - View as HTML
... West Phoenix, Arizona Michael Dorf, Attorney Michael Dorf, Attorney Michael Dorf, Attorney Michael Dorf, Attorney Adducci, Dorf, Lehner ...

Chicago law firm web pages
... A. Aberholden & Traurfeld, PC Abrahamson, Vorachek & Mikva Adducci, Dorf, Lehner, Mitchell & Blankenship, PC Aholm, Monahan, Keefe & Klaue Altheimer & Gray ...
www.kentlaw.edu/depts/cso/handout_Chicagofirmweb.html - 32k - Cached - Similar pages
Still no answer?
Netbios Backtrace Contd...
Still no answer?
Netbios Backtrace Contd...

Registrant:
Adducci, Dorf, Lehner, Mitchell & Blankenship (ADLMB-DOM)
150 N. Michigan Ave, Suite 2130
Chicago, IL 60601
US

Domain Name: ADLMB.COM

Administrative Contact:
Blankenship, Martin (MBM810)mblankenship@ADLMB.COM
Adducci, Dorf, Lehner, Mitchell & Blankenship
150 N. Michigan Ave, Suite 2130
Chicago, IL 60601
312.781.2800 (FAX) 312.781.7811

Technical Contact:
eLink Support (ES786-ORG)support@ELINKDC.COM
eLink Communications
6708 Wisconsin Avenue
Bethesda, MD 20815
US
240-744-1300
Fax- 240-744-1320

Record expires on 11-Dec-2002.
Record created on 11-Dec-2000.
Database last updated on 10-Jul-2002 21:21:15 EDT
If all else fails...

**Punt!**

Move 1 hop upstream as indicated by a traceroute and then repeat the whole backtracing process until you find a provider.
Get as close as possible

% This is the RIPE Whois server.
% The objects are in RPSL format.
% Please visit http://www.ripe.net/rpsl for more information.
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

inetnum: 62.220.108.0 - 62.220.111.255
netname: Intercompro
descr: Intercompro Communication Provider
country: IR
admin-c: HS400-RIPE
tech-c: HE81-RIPE
status: ASSIGNED PA
notify: registry@takta.net
mnt-by: TKT-MNT
mnt-lower: TKT-MNT
mnt-routes: TKT-MNT
changed: akbarshahi@takta.net 20011206
source: RIPE

route: 62.220.96.0/19
descr: Takta-Net
origin: AS21341
mnt-by: TKT-MNT
changed: akbarshahi@takta.net 20020107
...
Get as close as possible contd...

C:\nslookup
> set type=mx
> intercompro.net

*** No mail exchange (MX) records available for intercompro.net
> set type=a
> intercompro.net

*** No address (A) records available for intercompro.net
>
<table>
<thead>
<tr>
<th>Hop</th>
<th>Time</th>
<th>Time</th>
<th>Time</th>
<th>Host/Ip Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>&lt;10 ms</td>
<td>&lt;10 ms</td>
<td>10 ms</td>
<td>host121.mynetwatchman.com [64.238.113.121]</td>
</tr>
<tr>
<td>2</td>
<td>&lt;10 ms</td>
<td>&lt;10 ms</td>
<td>10 ms</td>
<td>172.16.41.165</td>
</tr>
<tr>
<td>3</td>
<td>&lt;10 ms</td>
<td>10 ms</td>
<td>&lt;10 ms</td>
<td>car00-s6-0-1.atlagabu.cbeyond.net [192.168.14.17]</td>
</tr>
<tr>
<td>4</td>
<td>&lt;10 ms</td>
<td>10 ms</td>
<td>&lt;10 ms</td>
<td>bgr00-g2-0.atlagabu.cbeyond.net [192.168.18.49]</td>
</tr>
<tr>
<td>5</td>
<td>&lt;10 ms</td>
<td>10 ms</td>
<td>&lt;10 ms</td>
<td>s1-0-0.ar1.ATL1.gblx.net [64.211.166.201]</td>
</tr>
<tr>
<td>6</td>
<td>&lt;10 ms</td>
<td>10 ms</td>
<td>10 ms</td>
<td>pos2-0-155M.cr2.ATL1.gblx.net [206.132.115.121]</td>
</tr>
<tr>
<td>7</td>
<td>30 ms</td>
<td>30 ms</td>
<td>20 ms</td>
<td>pos1-0-622M.cr2.NYC2.gblx.net [206.132.249.170]</td>
</tr>
<tr>
<td>8</td>
<td>20 ms</td>
<td>30 ms</td>
<td>20 ms</td>
<td>pos1-0-2488M.br2.NYC2.gblx.net [208.48.234.214]</td>
</tr>
<tr>
<td>9</td>
<td>20 ms</td>
<td>30 ms</td>
<td>20 ms</td>
<td>ftna.br2.NYC2.gblx.net [208.51.134.22]</td>
</tr>
<tr>
<td>10</td>
<td>20 ms</td>
<td>30 ms</td>
<td>20 ms</td>
<td>P10-0.NYKCR3.NY.opentransit.net [193.251.241.245]</td>
</tr>
<tr>
<td>11</td>
<td>20 ms</td>
<td>30 ms</td>
<td>20 ms</td>
<td>P11-0.NYKCR2.NY.opentransit.net [193.251.241.217]</td>
</tr>
<tr>
<td>12</td>
<td>100 ms</td>
<td>101 ms</td>
<td>100 ms</td>
<td>P4-0.PASCR1.Pstrl.opentransit.net [193.251.241.133]</td>
</tr>
<tr>
<td>13</td>
<td>100 ms</td>
<td>100 ms</td>
<td>110 ms</td>
<td>P3-0.PASCR3.Pstrl.opentransit.net [193.251.241.126]</td>
</tr>
<tr>
<td>14</td>
<td>100 ms</td>
<td>100 ms</td>
<td>110 ms</td>
<td>P9-0.PASBB1.Pstrl.opentransit.net [193.251.241.161]</td>
</tr>
<tr>
<td>15</td>
<td>101 ms</td>
<td>100 ms</td>
<td>110 ms</td>
<td>P8-0-0.PASAR1.Pstrl.opentransit.net [193.251.128.70]</td>
</tr>
<tr>
<td>16</td>
<td>100 ms</td>
<td>100 ms</td>
<td>101 ms</td>
<td>GlobeCastSerte.GW.opentransit.net [193.251.248.122]</td>
</tr>
<tr>
<td>17</td>
<td>100 ms</td>
<td>100 ms</td>
<td>100 ms</td>
<td>10.30.0.14</td>
</tr>
<tr>
<td>18</td>
<td>621 ms</td>
<td>631 ms</td>
<td>621 ms</td>
<td>62.220.96.125</td>
</tr>
<tr>
<td>19</td>
<td>631 ms</td>
<td>631 ms</td>
<td>621 ms</td>
<td>62.220.96.2</td>
</tr>
<tr>
<td>20</td>
<td>631 ms</td>
<td>620 ms</td>
<td>631 ms</td>
<td>62.220.100.7</td>
</tr>
<tr>
<td><strong>21</strong></td>
<td><strong>621 ms</strong></td>
<td><strong>621 ms</strong></td>
<td><strong>621 ms</strong></td>
<td><strong>62.220.101.131</strong></td>
</tr>
<tr>
<td>22</td>
<td>621 ms</td>
<td>631 ms</td>
<td>621 ms</td>
<td>62.220.111.241</td>
</tr>
</tbody>
</table>

Trace complete.
% This is the RIPE Whois server.
% The objects are in RPSL format.
% Please visit http://www.ripe.net/rpsl for more information.
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

netname: TAKTA-NET
descr: Takta Co. Access Service Provider
country: IR
admin-c: TR47-RIPE
tech-c: TR47-RIPE
status: ASSIGNED PA
mnt-by: TKT-MNT
mnt-lower: TKT-MNT
mnt-routes: TKT-MNT
changed: hostmaster@ripe.net 20011025
source: RIPE

route: 62.220.96.0/19
descr: Takta-Net
origin: AS21341
mnt-by: TKT-MNT
changed: akbarshahi@takta.net 20020107
source: RIPE
Conclusion
Are the calls coming from inside the house?

Unless you do Backtracing, you will never know the true source of an attack... or whether a packet was spoofed? However, even backtracing can't solve incorrect, non-existent, or just plain stale data present in some of the databases.
You **do** read your logs, right?

If not, consider having a service do it for you automatically, or use your own open-source tools to do it.

- [http://www.mynetwatchman.com](http://www.mynetwatchman.com)
- [http://www.dshield.org](http://www.dshield.org)
- Swatch
- Logsentry
References
“Avoiding future denial-of-service attacks” by Denise Pappalardo.
Posted on CNN.com February 23, 2000

Gan.ru. The Nuclear Regulatory Agency in Russia.
http://www.gan.ru

RFC 1812
http://www.faqs.org/rfcs/rfc1812.html

RFC 1918
http://www.faqs.org/rfcs/rfc1918.html

Solution to the Korean Spam Problem Example
http://www.merit.edu/mail.archives/nanog/2002-04/msg00029.html
http://www.merit.edu/mail.archives/nanog/2002-04/msg00044.html

“A Weakness in the 4.2BSD Unix† TCP/IP Software“ by Robert T. Morris

“NMAP: Decoy Analysis“ by Max Vision

Default TTL values.
http://216.239.35.100/search?q=cache:ybcsLpJuwSO:www.switch.ch/docs/ttl_default.html+NT+Default+TTL&hl=en&ie=UTF-8
Traceroute Hop Count Difficulties Example
http://www.merit.edu/mail.archives/nanog/2000-12/msg00143.html

Looking Glass Sites
http://lg.above.net/
http://nitrous.digex.net/cgi-bin/looking_glass.pl

Spoofed IP Example

Nslookup Example

Nice contact info here... Example

Regional NICs
http://www.arin.net
http://www.apnic.net
http://www.ripe.net

Geektools whois proxy.
http://www.geektools.com

Operational ICANN Accredited Domain Registrars
http://www.internic.net/alpha.html
“NeuStar Response to SB1335- 01-Q- 0740”
http://www.ntia.doc.gov/ntiahome/domainname/usca/cafiles/SectionE.pdf

Abuse Net
http://www.abuse.net

Rwhois
http://www.rwhois.net/

Success with RR Example

Gone Too Far? Example

Netbios Backtrace Example

Distributed IDSs
http://www.myNetWatchman.com
http://www.dshield.org
Appendix A:
ISP Anti-spoof Techniques
Ingress Filtering

“If an ISP is aggregating routing announcements for multiple downstream networks, strict traffic filtering should be used to prohibit traffic which claims to have originated from outside of these aggregated announcements.”

RFC2267 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
Input Debugging

Input Debugging allows an operator to filter particular packets on some egress port and determine which ingress port they arrived on. This reveals which upstream router originated the traffic.

The process is repeated recursively until the the ISP’s border is reached. From there, the upstream ISP must be contacted to continue the trace.
Backscatter

Backscatter Technique - “BGP implementations on Cisco and Juniper routers (possibly others) allow you to arbitrarily set the 'next-hop' to any IP address. This quirk can be used to your benefit when tracking spoofed traffic. By setting particular prefixes to a known and specially handled 'next-hop', we can get some unique traffic tracking information off the network.”