Using Sam Spade

Terry Pasley
GSEC Practical Assignment Version 1.4b

Abstract

In using the Internet, one often needs to determine where certain traffic comes from. The traffic might be a scan, a request for a web page, or an email. Since each packet contains a source IP number, by determining that number and who controls it one can obtain a great deal of information about the true meaning of the traffic. Once the "owner" of the IP address is determined appropriate action can be taken if the situation warrants.

A number of command-line tools were developed on UNIX systems during the early days of the Internet to assist in determining the source of Internet traffic. These tools include: whois, traceroute, finger, ping, and nslookup. While a number of these have been implemented in the various Windows operating systems, the Sam Spade utility provides all these tools and more in a graphical user interface. Sam Spade for Windows is free and available at www.samspade.org/ssw. This paper will examine a number of the more useful tools in Sam Spade.

Internet Protocol Number Background

IP numbers are used to route traffic across the Internet. With the exception of the "private IP addresses", all computers and router interfaces on the Internet have unique IP numbers (Atkins a). Although every host (computer or router interface) needs an IP number, you can't just make one up. An IP number assigned to a host must be a part of the proper range of IP numbers, which are assigned by various bodies responsible for large blocks of IP numbers.

Originally, all the possible IPv4 addresses were managed by the Internet Assigned Numbers Authority (http://www.iana.org/). Later, Regional Internet Registries (RIRs) were created. Each of the RIRs is responsible for managing IP address space in their own regions (http://www.aso.icann.org/rirs/). The RIRs further divide their ranges by placing blocks of IP addresses into the hands of National Internet Registries, which in turn place blocks in the hands of Local Internet Registries. These Local Internet Registries, which are often ISPs, in turn assign smaller blocks or individual addresses to companies and individuals who want Internet access. There are four RIRs at present:

ARIN: American Registry for Internet Numbers (North American, Africa south of the equator, and portions of the Caribbean) (http://www.arin.net/)

APNIC: Asia and Pacific Region (http://www.apnic.net/)

LACNIC: Latin America and portions of the Caribbean (http://www.lacnic.net/).

RIPE: Europe, Parts of Asia, Africa north of the equator, and the Middle East (http://www.ripe.net/).

There are numerous National Internet Registries that can be accessed from the above web sites. In the process of determining the owner of an IP number it is necessary to search the IP registration databases maintained by each Registry. This is done using the "whois" utility, which is discussed later in this paper. It is also sometimes useful to look at the entire IPv4 address space assignments. This can be found at http://www.iana.org/assignments/ipv4-address-space.

The assigned IP address is used in each packet sent from a host machine as the source address for the IP packet. This address is used to return response packets to a particular machine. Although there are ways to conceal the true source of a particular packet (using anonymous IP proxies), determining the person or entity controlling a particular address will often give you the true source of a packet, some idea of the intent of the packet, and someone to complain to if the intent of the packet is questionable.

Sam Spade

Sam Spade is a free utility containing tools to gather information on Internet hosts, analyze email headers, display web site code, and perform several other tasks. Sam Spade has been called the "Swiss Army Knife of network analysis" (Hiner). This paper will look at how to use some of these tools, such as Whois, Ping, IPBlock, Dig, Traceroute, Finger, Browse Web, and Parse email headers. Most of the functionality contained in Sam Spade is available in other utilities, usually command-line, but Sam Spade presents them all in a single graphical user interface that allows one to concentrate on the problem at hand and not worry so much about the different tools needed for the particular task one is working on. Sam Spade also has built-in logging capabilities that are very handy in chronicling an investigation. Sam Spade for Windows is free and available at http://www.samspade.org/ssw.

Getting Started with Sam Spade

The Sam Spade interface is composed of a menu bar, an address bar, a tool bar along the left side of the screen, a large "current" window, and a bar across the bottom of the screen where previous windows are accessible by clicking on them.

There are four boxes on a bar across the top of the Sam Spade window, under the menu bar. The first box on the left is the Address bar. This is the address that Sam Spade will apply the selected tool to. The other three boxes are part of the Options bar. First is a spin box allowing you to select the number of packets in a ping. Ten packets is the default. The next box is the Whois server text box. Several servers are pre-configured and more can be added to the list by editing the registry (Atkins b). The “Magic” setting lets Sam Spade make its best guess about which Whois server would be most appropriate for the given address. You can also add Whois servers directly to the text box, but these are not persistent. The final box is the DNS server to direct queries to. A default DNS server is configured under Edit, Options, Basic on the menu bar. DNS servers can also be added to this box.

The current window displays the results of executing a tool. Text displayed color coded and is either: Normal text, Comments, Warnings, Diagnostics, Hotlinks, Headings/Data, or Email Headers. By going to Edit on the menu bar, then Options, then clicking on the Colour tab you can customize the color of each. Right-clicking on a Hotlink will bring up a short menu based on what you could reasonably do with the type of Hotlink you clicked on. Left-clicking on a Hotlink will place it into the address box so you can continue applying tools to it.

Configuration

Most of the tools in Sam Spade will function correctly upon installation, but there are a few tools that require some configuration. The configuration dialog box is reached by clicking Edit on the menu bar, then Options. Some things you might want to configure are: a default name server, your email address, a web site (for dial-up connection keepalive, if needed), a network news server, a time server, and log file locations.

The Toolbar

There are a number of buttons along the left side of the screen. These are used to execute a number of the tools included in Sam Spade. The tools for looking up information about a remote host or domain are located on the Toolbar. Starting at the top, the important tools are:

> Two **Log** buttons: One logs and closes the current window (where the results of tool execution are displayed), the other simply logs without closing the current window. The window will then be available for future reference by clicking on buttons arranged in a bar under the current window. The logging function is particularly useful in organizing the results of an in-depth investigation.
>
> A **Copy** button and a **Paste** button.
>
> A **Ping** button: Sends a series of packets to the host indicated in the address box. The number of packets sent is configurable on the options bar. Used to verify basic network connectivity, but is not conclusive since a number of hosts are configured to not respond to ping requests.

A **DNS** button: Performs an nslookup on the host specified in the address bar. Used to resolve an IP number to a fully qualified domain name (FQDN) or to resolve an FQDN to an IP number.

A **Whois** button: Provides ownership and contact information for the host specified in the address bar. The whois request is run against the server specified in the Whois server box on the Options bar. Whois servers are maintained by the various Regional Internet Registries, National Internet Registries, etc. (Falk). Sam Spade offers a “Magic” option for the Whois server that will automatically refer the whois request to the most likely whois server. When investigating the ownership of an IP address it is sometimes necessary to add another whois server to the list on the Options bar, based on the results of previous whois queries.

An **IPBlock** button: A whois variation used to determine the ownership and contact information for a block of IP addresses. IPBlock is very useful when you can’t determine more specific information about a host. IPBlock is also useful in determining a host’s upstream Internet service provider (ISP). In the case of spam or illegal hacking the ISP can be contacted.

A **DIG** (Domain Internet Groper) button: DIG is an advanced Domain Name Service (DNS) tool that returns all of the available Resource Records for a given domain or host, including the start of authority (SOA) record, mail exchange (MX) records, and name server (NS) records. DIG can give you a starting point or can keep your investigation going in some situations.

A **Trace** button: Traceroute shows the route packets may take to the host specified in the Address bar (since the Internet is always in flux, actual packets might take a different route in some places). Good for determining the upstream providers of Internet service, and for identifying delays.

A **Finger** button: Finger obtains host/user information from a host running the finger daemon. Finger is usually disabled these days.

Using Sam Spade to Investigate an “Incident”

One day recently I had my laptop plugged into my work network. I received an alert from ZoneAlarm® that the laptop was being access on TCP Port 80, by a host at address 200.xxx.yyy.zzz. The laptop was not running WWW services, and our DHCP server issued the laptop’s IP number, so there was no legitimate reason for someone to think there was a web server at that IP address. ZoneAlarm® suggested this might be part of a Port 80 scan, so I checked the logs of a couple of our web servers and found the following:

```
200.xxx.yyy.zzz, -, 12/3/02, 11:18:38, W3SVC1, <mywebserver>,
<mywebserver IP address>, 16, 153, 623, 404, 3, GET,
scripts/..Á%8s../winnt/system32/cmd.exe,
/c+copy+c:\winnt\system32\cmd.exe+c:\inetpub\scripts\script.exe,
```

This seems to be an attack designed to exploit IIS's Unicode Directory Traversal vulnerability (Keane). The attack utilizes the fact that the default security permissions of the IIS scripts folder is Everyone can read, write, and execute files. The attack first attempts to create a copy of the Windows cmd.exe file in the c:\inetpub\scripts folder, and then to upload a file, such as netcat to the c:\inetpub\wwwroot folder. Netcat (Wysopal) would then provide a command prompt to anyone telnetting to Port 80, without any disruption of the www service.

Based on the above, I concluded that the web server's on my LAN were under attack and that I needed to determine the source of the attack. To do this I used Sam Spade. I started by entering the IP number of the attacker into the address bar and then clicking on the "Whois" button, using the Magic setting to let Sam Spade select the particular whois server to contact. Below is the result:

```
----------

12/11/02 11:03:46 IP block 200.xxx.yyy.zzz
Trying 200.xxx.yyy.zzz at ARIN
Trying 200.xxx.yyy at ARIN

OrgName:    Latin American and Caribbean IP address Regional Registry
OrgID:      LNIC

NetRange:   200.0.0.0 - 200.255.255.255
CIDR:       200.0.0.0/8
NetName:    LACNIC-200
NetHandle:  NET-200-0-0-0-1
Parent:
NetType:    Allocated to LACNIC
NameServer: ARROWROOT.ARIN.NET
NameServer: BUCHU.ARIN.NET
NameServer: CHIA.ARIN.NET
NameServer: DILL.ARIN.NET
NameServer: NS.LACNIC.ORG
NameServer: NS.DNS.BR
NameServer: NS2.DNS.BR
Comment:    This IP address range has been delegated to LACNIC.
            Please see http://www.lacnic.net/ for further details,
            or check the WHOIS server located at whois.lacnic.net
RegDate:    2002-07-27
```

```
Updated:    2002-11-18

TechHandle: LACNIC-ARIN
TechName:   Latin American and Caribbean IP address Regional R
TechPhone:  (+55) 11 5509-3525
TechEmail:  hostmaster@lacnic.net

OrgTechHandle: LACNIC-ARIN
OrgTechName:   Latin American and Caribbean IP address Regional R
OrgTechPhone:  (+55) 11 5509-3525
OrgTechEmail:  hostmaster@lacnic.net

# ARIN Whois database, last updated 2002-12-10 20:00
# Enter ? for additional hints on searching ARIN's Whois database.

-----------
```

Sam Spade went to ARIN with this initial whois request. From the results, we can see that the address in question is in the range delegated to the Latin American and Caribbean IP address Regional Registry (lacnic.net). Note that we are given name server information and technical contacts, but more importantly we are given the address of lacnic's whois server: whois.lacnic.net. I entered this into the whois server box on Sam Spade's Option bar (whois.lacnic.net was not one of the preconfigured whois servers available) and clicked the "Whois" button again:

```
----------

12/11/02 11:20:11 whois 200.xxx.yyy.zzz@whois.lacnic.net
whois -h whois.lacnic.net 200.xxx.yyy.zzz ...

% Copyright LACNIC lacnic.net
%  The data below is provided for information purposes
%  and to assist persons in obtaining information about or
%  related to AS and IP numbers registrations
%  By submitting a whois query, you agree to use this data
%  only for lawful purposes.
%  2002-12-11 14:20:05 (BRST -02:00)

inetnum:     200.128/9
status:      allocated
owner:       Comite Gestor da Internet no Brasil
ownerid:     BR-CGIN-LACNIC
responsible: <deleted by writer>
address:     <deleted by writer>
address:     <deleted by writer>
```

```
country:     BR
phone:       <deleted by writer> []
owner-c:     CGB
tech-c:      CGB
inetrev:     200.128/9
nserver:     NS.DNS.BR
nsstat:      20021209 AA
nslastaa:    20021209
nserver:     NS1.DNS.BR
nsstat:      20021209 AA
nslastaa:    20021209
nserver:     NS2.DNS.BR
nsstat:      20021209 AA
nslastaa:    20021209

remarks:     These addresses have been further assigned to Brazilian
users.
remarks:     Contact information can be found at the WHOIS server
located
remarks:     at whois.registro.br and at http://whois.nic.br
created:     19950104
changed:     20020902
nic-hdl:     CGB
person:      Comite Gestor da Internet no Brasil
e-mail:      <deleted by writer>
address:     <deleted by writer>
address:     <deleted by writer>
country:     BR
phone:       <deleted by writer> []
created:     20020902
changed:     20020902

% whois.lacnic.net accepts only direct match queries.
% Types of queries are: POCs, ownerid, CIDR blocks, IP
% and AS numbers.

----------
```

The whois server at lacnic reports the IP number in question has been further delegated to the country of Brazil. Note that I have deleted addresses and contact information from the output. Also note that from the line:

```
inetnum:     200.128/9
```

we are not yet to the subnet of the attacking machine (since I am not showing you the whole attacking IP number, you will have to take my word for this). We do have the Brazilian whois server, whois.registro.br, to consult. I entered this into Sam Spade’s whois server box and clicked the “Whois” button again:

```
----------

12/11/02 11:40:09 whois 200.xxx.yyy.zzz@whois.registro.br
whois -h whois.registro.br 200.xxx.yyy.zzz ...

% Copyright registro.br
%  The data below is provided for information purposes
%  and to assist persons in obtaining information about or
%  related to domain name and IP number registrations
%  By submitting a whois query, you agree to use this data
%  only for lawful purposes.
%  2002-12-11 14:40:04 (BRST -02:00)

inetnum:     200.xxx.yyy/21
aut-num:     <deleted by writer>
abuse-c:     <deleted by writer>
owner:       <deleted by writer>
ownerid:     <deleted by writer>
responsible: <deleted by writer>
address:     <deleted by writer>
address:     <deleted by writer>
phone:       <deleted by writer> []
owner-c:     <deleted by writer>
tech-c:      <deleted by writer>
created:     20021111
changed:     20021111
inetnum-up:  200.xxx.0/17

nic-hdl-br:  <deleted by writer>
person:      <deleted by writer>
e-mail:      <deleted by writer>
address:     <deleted by writer>
address:     <deleted by writer>
phone:       (<deleted by writer>
created:     19981005
changed:     20020214

nic-hdl-br:  <deleted by writer>
person:      <deleted by writer>
e-mail:      <deleted by writer>
address:     <deleted by writer>
address:     <deleted by writer>
phone:       <deleted by writer>
```

```
created:     20000502
changed:      20020401

remarks:     Security issues should also be addressed to
remarks:     <deleted by writer>, http:// <deleted by writer>
remarks:     Mail abuse issues should also be addressed to
remarks:     mail-abuse@<deleted by writer>

% whois.registro.br accepts only direct match queries.
% Types of queries are: domains (.BR), BR POCs, CIDR blocks,
% IP and AS numbers.

----------
```

We now have what appears to be a “local” ISP. From the subnet mask of /21 we can determine that this ISP is responsible for 2^{11} or about 2,000 IP numbers. We also have contact information, including email addresses. I emailed one of the technical contacts with the information I had collected about this incident, which is standard procedure in these cases. I received a reply that he would check into it.

In the process of using Sam Spade I have determined that an investigation doesn’t always play out exactly this way. Sometimes it only takes a couple of tool clicks to go as far as you can go. Sometimes it’s much more involved. For any particular investigation you have to read the results as you go and let the results determine where you go next. I have also tried to determine whether it is better to do a whois on the host IP address or to do an IPBlock (IPBlock is based on whois). I see no difference in the cases I have looked at so far.

I have also tried to determine whether any of the other tools, such as DIG or nslookup, would serve as a more appropriate route in the investigation. Here is the output for the same IP number using DIG:

```
----------

12/11/02 14:56:59 dig 200.xxx.yyy.zzz @ <my DNS server>
Dig zzz.yyy.xxx.200.in-addr.arpa@<my DNS server> ...
Non-authoritative answer
Recursive queries supported by this server
 Query for zzz.yyy.xxx.200.in-addr.arpa type=255 class=1
  xxx.200.in-addr.arpa SOA (Zone of Authority)
        Primary NS: <deleted by writer>
        Responsible person: <deleted by writer>
        serial: <deleted by writer>
        refresh:7200s (2 hours)
        retry:3600s (60 minutes)
        expire:604800s (7 days)
        minimum-ttl:86400s (24 hours)

----------
```

This isn’t terribly helpful as a starting point. Nslookup is no better:

```
----------

12/11/02 15:07:09 dns 200.xxx.yyy.zzz
nslookup 200.xxx.yyy.zzz
No reverse DNS (WSANO_DATA)

----------
```

This just tells us there is no reverse DNS record (IP to Hostname mapping) available for the IP number in question. This does lead one to believe the address was being used by a workstation, perhaps a dial-up, because servers usually have reverse DNS records (technically called pointer, or PTR records). Of course this is just supposition on my part.

Sam Spade and Email

Sam Spade also has a number of tools to apply to email in general, and to spam in particular. Spam, or unwanted email sent to hundreds or thousands of recipients, takes up server space, eats up our bandwidth, annoys the users, and is a security issue when the emails contain attachments with viruses. The tools for dealing with spam are found under Basics and Tools on the menu bar and include (Kessler):

> **SMTP VRFY**: Used to verify whether an email address is a true address or is being forwarded.
>
> **SMTP Relay check**: Used to determine if a particular mail server will relay mail (pass the mail on to another server). You can use this to verify that your mail server is properly set to not relay mail.
>
> **Blacklist lookups and Abuse.net query**: Two related tools that allow you to check web sites that keep track of known spammers.
>
> **E-mail header analysis**: Used to analyze the headers of an email address to determine where it really came from. Breaks an email header down and allows the other investigative tools such as whois to be used on hosts and domains found in the email header.

Email headers

A number of computers handle every email you send, typically a minimum of four computers: your computer, your email server, the email server of the recipient, and the recipient's computer. Various (legitimate) headers are put on by the first three machines, and forged and/or misleading headers can also be added (Lucke). While a complete discussion of email headers and the ways they can be manipulated is beyond the scope of this paper, there are some basic steps that happen. The first header is put on by the mail client on your machine, the second by your mail server, and a third by the mail server of the person you are mailing. It looks like this at your mail client:

> From header:
> Email message: xxxxxxxxxxxxxxxxxxxxxxxxx
> xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

At your mail server another header is added:

> From mail server (sender's mail server)
> From header:
> Email message: xxxxxxxxxxxxxxxxxxxxxxxxx
> xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

After going through the destination mail server:

> From mail server (recipient's mail server)
> From mail server (sender's mail server)
> From header:
> Email message: xxxxxxxxxxxxxxxxxxxxxxxxx
> xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Note that each successive header is added to the front of the message.

It is possible to introduce bogus information at both the sender's mail client and at the sender's mail server (or servers). One way of introducing misleading information is by included text that looks like a header as part of the message:

> From header:
> Text that looks like header, but is really part of the message.
> Rest of the email message: xxxxxxxxxxxxxxxxxxxxxxxxx
> xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

This bogus From header would then be displayed by the mail client. The sender's mail server could also add erroneous information in the From: header, pretending to be someone else for example.

Normally your mail client is rather unsophisticated in its interpretation of the headers on a received message. That's why a message that appears to be from someone often turns out to be from someone else. Of course, this is the plan. The message is supposed to appear to be something you would want to read instead of just deleting. Since most mail clients have a mechanism for showing you the headers (Muth b) you can analyze the headers yourself, but Sam Spade's tools make this much easier. Let's start with a typical email header:

```
  ---- Forwarded message ----
> Received: from mx3.hotmail.com (80.xxx.yyy.zzz [80.xxx.yyy.zzz]) by
<mymailserver> with SMTP (Microsoft Exchange Internet Mail Service
Version 5.5.2656.59)
>        id YLRDD6XP; Sat, 7 Dec 2002 06:20:42 -0500
> From: Bruno <Bruno@hotmail.com>
> To: <terry.pasley@mydomain.com>
> Subject: i am getting new ones on monday
> MIME-Version: 1.0
> Content-Type: text/html; charset="US-ASCII"
> Content-transfer-encoding: 7bit
```

This header claims the message is from someone at hotmail.com. Note the claim the message was received from mx3.hotmail.com (80.xxx.yyy.zzz [80.xxx.yyy.zzz]). My mail server also noted the source IP number on the packets containing the message. Let's use Sam Spade to see what's really going on here. First, select and copy the header, then paste it into Sam Spade's "Parse Email Headers" tool. After clicking parse, we get the following output (the original output is in color, and I have done some formatting to distinguish certain parts of the output so I don't have to reproduce the colors, which could be a problem for some readers):

```
----------

12/11/02 21:28:32 Input
        The Received: headers are the important ones to read

        My comments are just hints, and should be considered only
        an opinion. I may have guessed wrong, or things may have
        changed since I was written

Received: from mx3.hotmail.com (80.xxx.yyy.zzz
   [80.xxx.yyy.zzz]) by <mymailserver> with SMTP
   (Microsoft Exchange Internet Mail Service Version
   5.5.2656.59) id YLRDD6XP; Sat, 7 Dec 2002 06:20:42 -0500
          This received header was added by your mailserver
          <mymailserver> received this from someone claiming
          to be mx3.hotmail.com but really from 80.xxx.yyy.zzz(No rDNS)

          All headers below may be forged


From: Bruno <Bruno@hotmail.com>
          Many spams are forged to appear connected to hotmail.com. They
          probably aren't from there. If the spam is soliciting replies to a
          hotmail.com address tell abuse@hotmail.com and the mailbox will
          die.

To: <terry.pasley@mydomain.com>
Subject: i am getting new ones on monday
MIME-Version: 1.0
Content-Type: text/html; charset="US-ASCII"
Content-transfer-encoding: 7bit

----------
```

Notice from the indented comments that the email purports to be from someone at hotmail.com, but Sam Spade checks the forwarding mail server name against the source IP number of the message (80.xxx.yyy.zzz) and determines they don’t match. Next I click on 80.xxx.yyy.zzz, which places the address into the address bar. Now I can use the Sam Spade tools to determine who 80.xxx.yyy.zzz really belongs to. Using whois and the “Magic” setting:

```
----------

12/15/02 09:19:57 IP block 80.xxx.yyy.zzz
Trying 80.xxx.yyy.zzz at ARIN
Trying 80.48.123 at ARIN

OrgName:    RIPE Network Coordination Centre
OrgID:      RIPE

NetRange:   80.0.0.0 - 80.255.255.255
CIDR:       80.0.0.0/8
NetName:    80-RIPE
NetHandle:  NET-80-0-0-0-1
Parent:
NetType:    Allocated to RIPE NCC
NameServer: NS.RIPE.NET
NameServer: AUTH62.NS.UU.NET
NameServer: NS3.NIC.FR
NameServer: SUNIC.SUNET.SE
NameServer: MUNNARI.OZ.AU
```

```
NameServer: NS.APNIC.NET
NameServer: SVC00.APNIC.NET
Comment:    These addresses have been further assigned to users in
         the RIPE NCC region. Contact information can be found in
         the RIPE database at whois.ripe.net

RegDate:
Updated:    2002-09-11

OrgTechHandle: RIPE-NCC-ARIN
OrgTechName:   RIPE NCC Hostmaster
OrgTechPhone:  +31 20 535 4444
OrgTechEmail:  nicdb@ripe.net

# ARIN Whois database, last updated 2002-12-14 20:00
# Enter ? for additional hints on searching ARIN's Whois database.

----------
```

Again, we need to check a whois server closer to the machine in question, so I'll use whois again, this time using the ripe.net whois server:

```
----------

12/15/02 09:32:29 whois 80.xxx.yyy.zzz@whois.ripe.net

whois -h whois.ripe.net 80.xxx.yyy.zzz ...
% This is the RIPE Whois server.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-services/db/copyright.html

inetnum:     80.xx.yyy.0 - 80.xx.yyy.255
netname:      <deleted by writer>
descr:       <deleted by writer>
descr:       Lodz
country:      PL
admin-c:      <deleted by writer>
tech-c:      <deleted by writer>
status:      ASSIGNED PA
mnt-by:       <deleted by writer>
changed:      <deleted by writer>
source:       RIPE

route:       80.xx.0.0/13
```

```
descr:        <deleted by writer>
descr:        Provider Local Registry
origin:       <deleted by writer>
notify:       <deleted by writer>
mnt-by:       <deleted by writer>
changed:      <deleted by writer>
source:       RIPE

person:       <deleted by writer>
address:      <deleted by writer>
address:      <deleted by writer>
address:      <deleted by writer>
address:      Poland
phone:        <deleted by writer>
fax-no:       <deleted by writer>
e-mail:       <deleted by writer>
nic-hdl:      <deleted by writer>
mnt-by:       <deleted by writer>
changed:      <deleted by writer>
source:       RIPE

person:       <deleted by writer>
address:      <deleted by writer>
address:      <deleted by writer>
address:      <deleted by writer>
address:      POLAND
phone:        <deleted by writer>
fax-no:       <deleted by writer>
e-mail:       <deleted by writer>
nic-hdl:      <deleted by writer>
mnt-by:       <deleted by writer>
changed:      <deleted by writer>
source:       RIPE

---------
```

So the email message is not from someone at hotmail after all, but from a company in Poland. At this point you would use Sam Spade to check the source of the message to see if it's listed in the MAPS (Mail Abuse Prevention System) mail abuse database (Muth a). For the email above, nothing was found. There is also an abuse email button in Sam Spade that will check whois.abuse.net for an email address to direct complaints to:

```
----------
```

```
12/15/02 09:59:21 Abuse address lookup for <deleted by writer>

whois -h whois.abuse. <deleted by writer>...
abuse@<deleted by writer>

----------
```

You could also report unwanted or deceptive messages to the Federal Trade Commission, who maintains a database of such messages to pursue law enforcement actions against people who send deceptive email (http://www.ftc.gov/bcp/conline/pubs/online/inbox.htm).

Web Tools

Sam Spade also contains a web crawler that will list all the linked pages in a web site, and a web browsing tools that will show you the html for a web page. These tools are very handy in investigating a web site that could have less than honorable intentions.

Sam Spade Online Tools

There is also an online version of several of the tools available at http://www.samspade.org/t/. The online tools are handy in those cases you are working at a different computer from your usual workstation or if you are working behind a restrictive firewall. I noticed that several of the installed tools will not work if you are running ZoneAlarm®, for example. There are some issues with the online tools, however. When doing a whois using the "Magic" setting (explained later) I repeatedly received the following message:

> SamSpade.org is being null-routed by ARIN due to high traffic. This service will not be available until that is resolved. Please do not contact ARIN about this.

When I tried a whois to apnic.net I received the following message:

```
% [whois.apnic.net node-2]
%ERROR:201: access denied%
% Access from your host has been permanently denied due to
% repeated excessive querying of the database. To reinstate
% your host's access to the database please see:
%     http://www.apnic.net/db/dbcopyright.html
```

Apparently some of the whois servers are blocking/ignoring requests made through the Sam Spade online whois tool. There may be other such issues.

Conclusion

While there is nothing in Sam Spade that you can't do other ways or from other sources, the combination of the tools, their ease of use and integration into a clean, functional GUI, running in the Windows environment, makes Sam Spade a very attractive package. Sam Spade can help you with several of your day-to-day tasks as a security professional, and the fact that it is free only makes it more attractive.

References:

Atkins, Steve a. "Internet Protocol Addressing." http://www.samspade.org/d/ipdns.html.

Atkins, Steve b. "Things you should know." http://www.samspade.org/ssw/tips.html.

Falk, Ed. "Notes on whois." http://www.rahul.net/falk/whois.html.

Federal Trade Commission. "You've Got Spam: How to "Can" Unwanted Email." April 2002. http://www.ftc.gov/bcp/conline/pubs/online/inbox.htm.

Hiner, Jason. "Sam Spade: The Swiss Army Knife of network analysis." 20 December 2000. http://libra.unitbv.ro/internet/tools/samspade.htm.

Keane, Justin. "IIS Unicode Directory Traversal Exploit Explained." 2002. http://www.madirish.net/tech.php?section+7&article=57.

Kessler, Gary. "Sam Spade: A Multifunction Information Toolkit." May 2001. http://www.garykessler.net/library/is_tools_sam_spade.html.

Lucke, Ken. "Reading Email Headers." 1997. http://www.stopspam.org/email/headers/headers.html.

Muth, Doug a. "Blocking Spam." http://www.claws-and-paws.com/spam-l/blocking.html.

Muth, Doug b. "Tracking Spam." http://www.claws-and-paws.com/spam-l/tracking.html.

Wysopal, Chris. "Netcat 1.10 for NT - nc11nt.zip." 2 February 1998. http://www.atstake.com/research/tools/nc11nt.txt.