

## ***Learn Information Gathering By Example***

**Aelphaeis Mangarae [IRC.EFnet.Org #d-u]**

**July 11<sup>th</sup> 2006**



<http://www.SecurZone.org>

**Join Aelphaeis Mangarae On IRC:**

[#d-u">\*\*irc.EFnet.org #d-u\*\*](irc.EFnet.org)

**© Copyright Aelphaeis Mangarae 2006**

## **Table Of Contents**

**Introduction**

**Utilizing Search Engines**

**Utilizing NetCraft**

**Using Whois**

**Utilizing NSLookup**

**Brute Forcing DNS Names**

**Performing A Ping Sweep**

**Identifying Firewalls/Routers**

**Gathering Information From Emails**

**Obtaining Information With Scripts**

**About The Author**

**Greetz To**

## **Introduction**

Information Gathering is usually the first done when Penetration testing. It is indeed a very important part in Penetration testing, and no Penetration tester or Internet security enthusiast can be left without the knowledge of not knowing how to successfully gather information on a target. This white paper goes through the steps and tools you can use in order to successfully gather information on a target web server.

## Utilizing Search Engines

Search Engines can be used (In particular Google) to gather information on a target host.

The first and probably most powerful search string in Google is the “site:” string.  
This will give us all of the pages that have been indexed by Google, this can be used to gather sub domains.  
Although this can usually be gathered through other means, using Google is an effective and **anonymous** way of getting this sort of information.

The screenshot shows a Mozilla Firefox browser window with the title bar "site:boeing.com - Google Search - Mozilla Firefox". The address bar contains the URL "http://www.google.com.au/search?hl=en&q=site%3Aboeing.com&btnG=Google+Search&meta=". The search query "site:boeing.com" is entered in the search bar. Below the search bar, there are options for "Web", "Images", "Groups", "News", and "more ». The search button is labeled "Search" and has links to "Advanced Search Preferences". The results section shows the number of results: "Results 1 - 50 of about 281,000 from boeing.com for . (0.17 seconds)". The first result is "The Boeing Company", followed by "Jobs Boeing.com - Jobs Boeing.Com Home", "Boeing: Integrated Defense Systems - Delta Launch Vehicles", "Boeing Employment: Featured Opportunities", and "Rocketdyne Worker Health Study". Each result includes a link, file size (e.g., 117k, 14k, 15k), and links to "Cached" and "Similar pages". At the bottom left, there is a "Done" button.

As you can see the second listing down gives us a Boeing sub domain “jobs.boeing.com”. If you search “site:boeing.com” in Google and scroll down you will find more sub domains.

Some other interesting queries are:

link:targethost.com  
"Company Name Here"  
Email Addresses (Obtained from the website or Whois Database.)  
Forum Usernames

You may be wondering why search Email Addresses and Forum Usernames? Well the concept is quite simple. It is very possible that the administrators talk on Forums, possibly to get help with their website. The posts they make on the Forums may contain information relating to the website. It is also possible (If the admin is incompetent enough) that they may use the same password for numerous things. Hence obtaining their forum password would be very useful.

## Utilizing NetCraft

NetCraft can be a very useful tool in Penetration testing, as it often delivers a lot of information on the target host.

Site report for www.zone-h.org				
<b>Site</b>	<a href="http://www.zone-h.org">http://www.zone-h.org</a>	<b>Last reboot</b>	unknown	 <a href="#">Uptime graph</a>
<b>Domain</b>	zone-h.org	<b>Netblock owner</b>	Serverhousing	
<b>IP address</b>	213.219.122.11	<b>Site rank</b>	3032	
<b>Country</b>	 EE	<b>Nameserver</b>	ns1.register.it	
<b>Date first seen</b>	March 2002	<b>DNS admin</b>	hostmaster@register.it	
<b>Domain Registry</b>	publicinterestregistry.net	<b>Reverse DNS</b>	www.zone-h.org	
<b>Organisation</b>	As Domina Privacy & Security, Suur Patarei 3, Tallin, 10415, Estonia	<b>Nameserver Organisation</b>	REGISTER.IT S.p.a., Italy	
<b>Check another site:</b>	<input type="text"/>			
Hosting History				
<b>Netblock Owner</b>	<b>IP address</b>	<b>OS</b>	<b>Web Server</b>	<b>Last changed</b>
Serverhousing Sole 14 Tallinn Estpak Data/Estonian Telephone Co	213.219.122.11	NetWare	Apache/2.0.49a NETWARE PHP/4.2.4-dev mod_jk/1.2.6-dev	3-Apr-2006
Serverhousing Sole 14 Tallinn Estpak Data/Estonian Telephone Co	213.219.122.11	Windows Server 2003	Microsoft-IIS/6.0	18-Mar-2006
Serverhousing Sole 14 Tallinn Estpak Data/Estonian Telephone Co	213.219.122.11	Windows Server 2003	Microsoft-IIS/6.0	17-Mar-2006
Serverhousing Sole 14 Tallinn Estpak Data/Estonian Telephone Co	213.219.122.11	unknown	Apache/1.3.33 Darwin PHP/4.3.10	16-Mar-2006
Serverhousing Sole 14 Tallinn Estpak Data/Estonian Telephone Co	213.219.122.11	Linux	Apache	14-Mar-2006
Serverhousing Sole 14 Tallinn Estpak Data/Estonian Telephone Co	213.219.122.11	unknown	Apache/1.3.33 Darwin PHP/4.3.10	13-Mar-2006

NetCraft can give you information such as:

- \*A history of web servers used by the target host.
- \*A history of Operating Systems used by the target host.
- \*Approximate times of when web server software, Operating System or host have been changed.
- \*The owner of the target host.
- \*IP Address of the target host.

The information provided by NetCraft would be useful in knowing for many reasons.  
Information on the web server used by the target host as well as the Operating System can be used to be able to work out what vulnerabilities the host would have.  
If the target host seems to be moving servers a lot it may be because his website is mirrored on two or more servers.

## Using Whois

A Whois is a target host can be done using many software applications and websites. For this paper I am going to use some websites to do a Whois on a target host. Using the Domain Dossier at Central Ops (<http://centralops.net/co/>) we able to gather a lot of important information on our target host.

The screenshot shows the 'Domain Dossier' interface. At the top, it says 'Investigate domains and IP addresses'. Below that is a search bar containing 'chasenet.org'. There are several checkboxes: 'domain whois record' (checked), 'DNS records' (checked), 'traceroute' (unchecked), 'network whois record' (checked), and 'service scan' (unchecked). A 'go' button is next to the service scan checkbox. At the bottom left, it says 'user: 202.134.235.32 [anonymous] 50/50' with links 'log in | get account'. On the right, it says 'Central Ops.net'.

Using Domain Dossier we can do a Whois on our target (Chasenet.org.) If we want we can also do a basic service scan and a traceroute.

By using Domain Dossier we were able to get information on Domain (General Whois Information), Network Information as well as DNS records.

After doing a Whois you should look for things of importance, such as:

- \*Registrant Name
- \*Registrant Organization
- \*Registrant Street, City, Town, Country, Postal Code
- \*Registrant Phone and/or Fax number(s)
- \*Email Addresses (Useful for Social Engineering, along with other details)
- \*Name Servers (Useful for **Zone Transfers**)
- \*Mail Servers (Might be useful for faking/spoofing mail)
- \*IP Block/Range (This will be needed to conduct a **Ping Sweep**)

For people who wish to do a Whois on a domain that doesn't seem be bring up any information (using Domain Dossier) you would want to use a region specific Whois database. These would also be useful when doing a Reverse DNS.

Europe:

<http://www.ripe.net/perl/whois/>

Asia Pacific Region:

<http://www.apnic.net/apnic-bin/whois.pl>

Latin American and Caribbean:

<http://www.lacnic.net/cgi-bin/lacnic/whois>

## **www.SecurZone.Org**

---

African And Indian Ocean:

<http://www.afrinic.net/cgi-bin/whois>

North America:

<http://www.arin.net/whois/>

Military Whois:

<http://www.nic.mil/dodnic/>

Government Whois:

<http://www.igotit.cc/usgov.html>

## Utilizing NSLookup

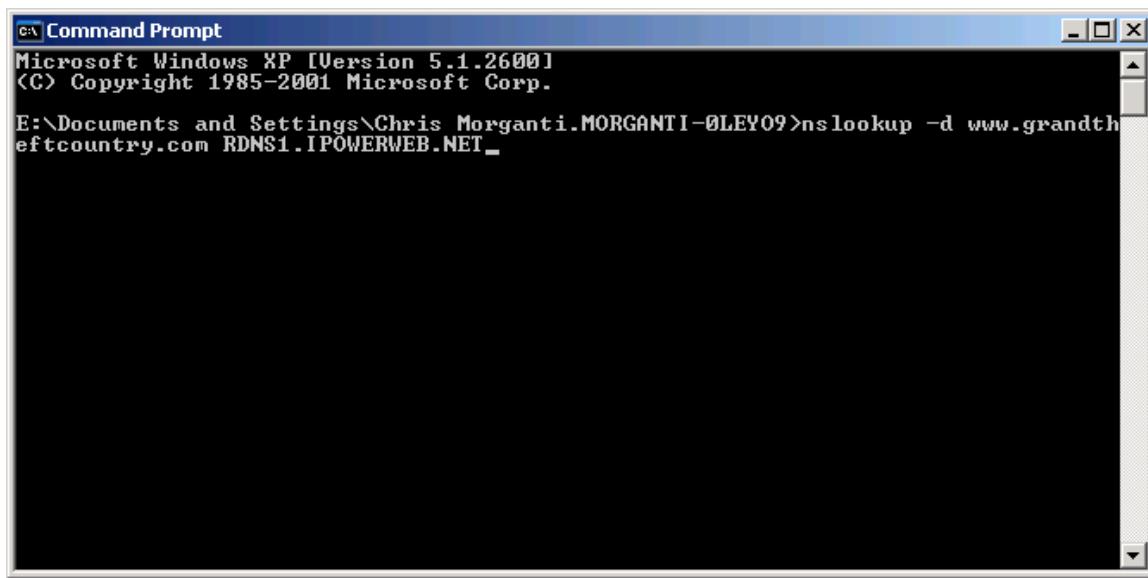
### What Is NSLookup?

NSLookup is simply a tool that can be used to gather information on a target **via a Zone Transfer**. This information can be useful when doing Information Gathering during a Penetration Test.

Before we begin I will explain some of the switches (options) that can be used with NSLookup.

- t Lists all records of the type specified. (In the Windows version of NSLookup it says this is an invalid option, so just use the other options by themselves.)
- a Lists all of the aliases for the hosts in the domain.
- h Lists CPU and Operating System information for the domain.
- s Lists well-known services of hosts in the domain.
- d Lists all records for the domain.

Let's now do a Whois on a target.



```
C:\Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\Documents and Settings\Chris Morganti.MORGANTI-OLEY09>nslookup -d www.grandth
eftcountry.com RDNS1.IPOWERWEB.NET
```

Here is the information NSLookup gave me on the target host:

**Note: Notice I had to give NSLookup a Name Server to use, you will have to do this too when using NSLookup (well I would recommend doing it anyway.)**

# [www.SecurZone.Org](http://www.SecurZone.Org)

---

Got answer:

HEADER:

```
opcode = QUERY, id = 1, rcode = NOERROR
header flags: response, auth. answer, want recursion, recursion avail.
questions = 1, answers = 1, authority records = 1, additional = 1
```

QUESTIONS:

```
64.200.235.66.in-addr.arpa, type = PTR, class = IN
```

ANSWERS:

```
-> 64.200.235.66.in-addr.arpa
name = rdns1.ipowerweb.net
ttl = 3600 (1 hour)
```

AUTHORITY RECORDS:

```
-> 200.235.66.in-addr.arpa
nameserver = rdns2.ipowerweb.net
ttl = 3600 (1 hour)
```

ADDITIONAL RECORDS:

```
-> rdns2.ipowerweb.net
internet address = 66.235.216.64
ttl = 1052 (17 mins 32 secs)
```

---

```
-----  
Server: rdns1.ipowerweb.net  
Address: 66.235.200.64
```

Got answer:

HEADER:

```
opcode = QUERY, id = 2, rcode = NOERROR
header flags: response, want recursion, recursion avail.
questions = 1, answers = 1, authority records = 4, additional = 4
```

QUESTIONS:

```
www.grandtheftcountry.com, type = A, class = IN
```

ANSWERS:

```
-> www.grandtheftcountry.com
internet address = 72.22.69.19
ttl = 3523 (58 mins 43 secs)
```

AUTHORITY RECORDS:

```
-> grandtheftcountry.com
nameserver = ns1.ipowerweb.net
ttl = 3523 (58 mins 43 secs)
```

```
-> grandtheftcountry.com
nameserver = ns1.ipowerdns.com
ttl = 3523 (58 mins 43 secs)
```

```
-> grandtheftcountry.com
nameserver = ns2.ipowerweb.net
ttl = 3523 (58 mins 43 secs)
```

```
-> grandtheftcountry.com
nameserver = ns2.ipowerdns.com
ttl = 3523 (58 mins 43 secs)
```

ADDITIONAL RECORDS:

```
-> ns1.ipowerweb.net
internet address = 64.70.61.130
ttl = 136245 (1 day 13 hours 50 mins 45 secs)
```

```
-> ns1.ipowerdns.com
internet address = 66.235.217.202
ttl = 114042 (1 day 7 hours 40 mins 42 secs)
```

```
-> ns2.ipowerweb.net
internet address = 66.235.217.200
ttl = 136245 (1 day 13 hours 50 mins 45 secs)
```

```
-> ns2.ipowerdns.com
internet address = 64.70.61.131
ttl = 117643 (1 day 8 hours 40 mins 43 secs)
```

---

```
-----  
Non-authoritative answer:
```

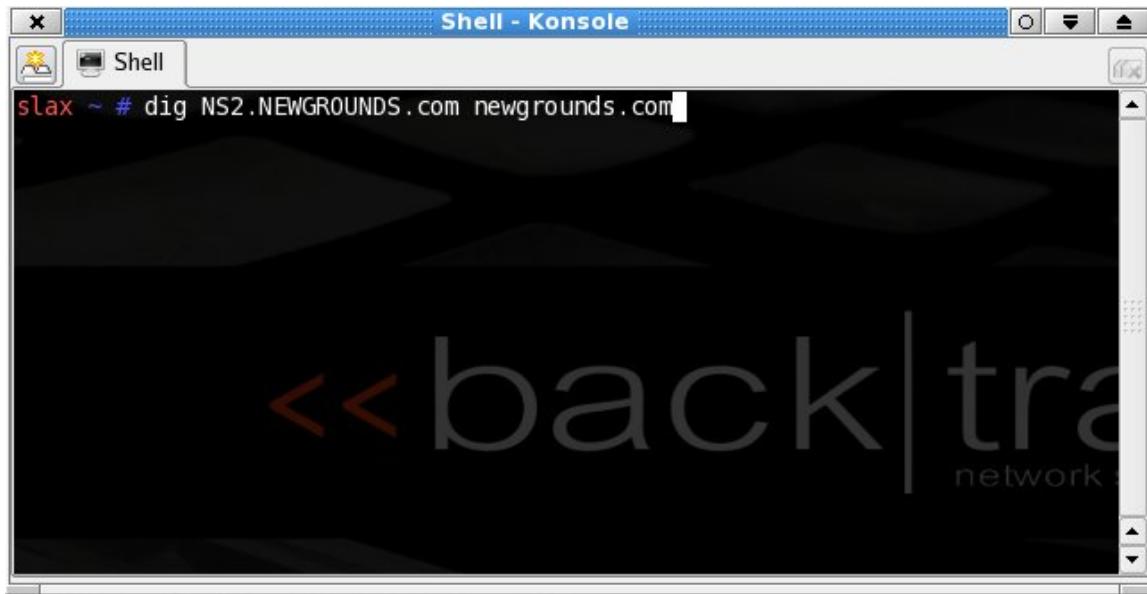
```
Name: www.grandtheftcountry.com
```

```
Address: 72.22.69.19
```

If you don't wish to use the UNIX or Windows command line NSLookup you do have the option of using a web based one (How good each of these are I don't know.)

<http://www.kloth.net/services/nslookup.php>  
<http://www.zoneedit.com/lookup.html>  
<http://www.webmaster-toolkit.com/ns-lookup.shtml>  
<http://www.bankes.com/nslookup.htm>  
<http://www.infobear.com/nslookup.shtml>

The Linux equivalent of NSLookup is Dig.



Usage: dig @NameServer host.com

Result:

A screenshot of a Kali Linux desktop environment. In the foreground, there is a terminal window titled "Shell - Konsole <2>". The terminal displays the output of a "dig" command. The output shows the following details:

```
; <>> DiG 9.3.1 <>> @NS2.NEWGROUNDS.COM newgrounds.com
; (1 server found)
; global options: printcmd
; Got answer:
; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 15153
; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 5
; QUESTION SECTION:
;newgrounds.com.           IN      A
;ANSWER SECTION:
newgrounds.com.        86400   IN      A      38.119.130.61
; AUTHORITY SECTION:
newgrounds.com.        86400   IN      NS     ns1.newgrounds.com.
newgrounds.com.        86400   IN      NS     ns2.newgrounds.com.
newgrounds.com.        86400   IN      NS     auth1.dns.cogentco.com
newgrounds.com.        86400   IN      NS     auth2.dns.cogentco.com
newgrounds.com.        86400   IN      NS     auth3.dns.cogentco.com
```

The background shows the Kali Linux desktop with its characteristic orange and black "backtrack" logo.

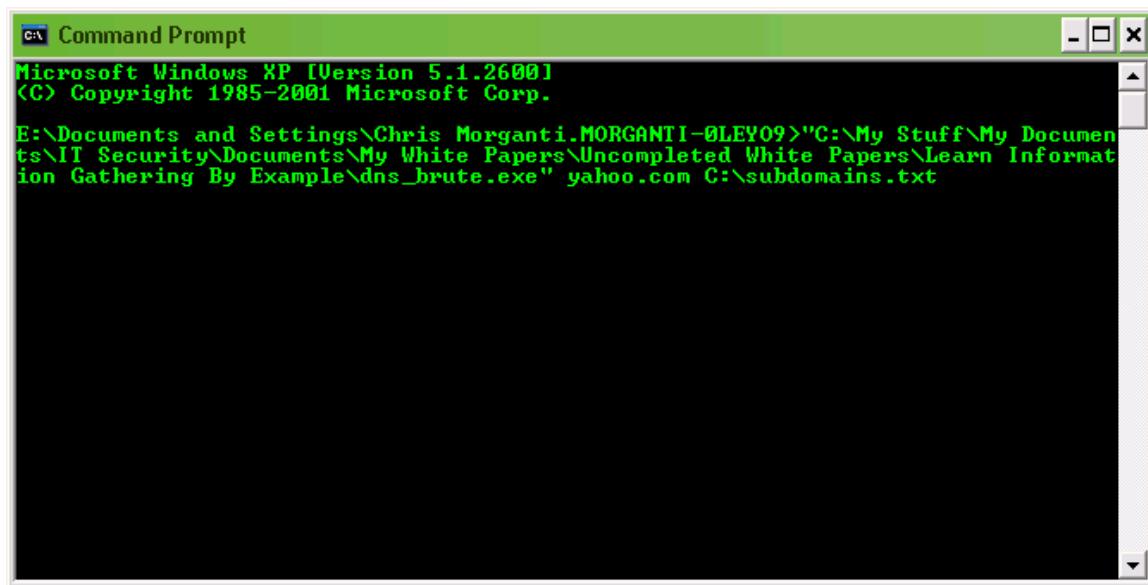
With these particular servers we haven't really had any luck retrieving any sub domains.  
**What information you get will vary from server to server, depending on how they are configured.**

## Brute Forcing DNS Names

We have tried some ways of obtaining sub domains for attacking. But how about brute forcing them? Well this is of course possible. I set out to find a program that I could use to do such a thing. Unfortunately I didn't find any. So I decided to code my own that could brute force sub domains of a domain.

All I needed to do was code a program that pinged each sub domain to see if they were alive. Although I am aware that it is of course possible that some sub domain's will not reply to ICMP packets therefore making this piece of software I coded (**DNS Brute**) useless. However it isn't that likely that a group of servers are going to be set up that way.

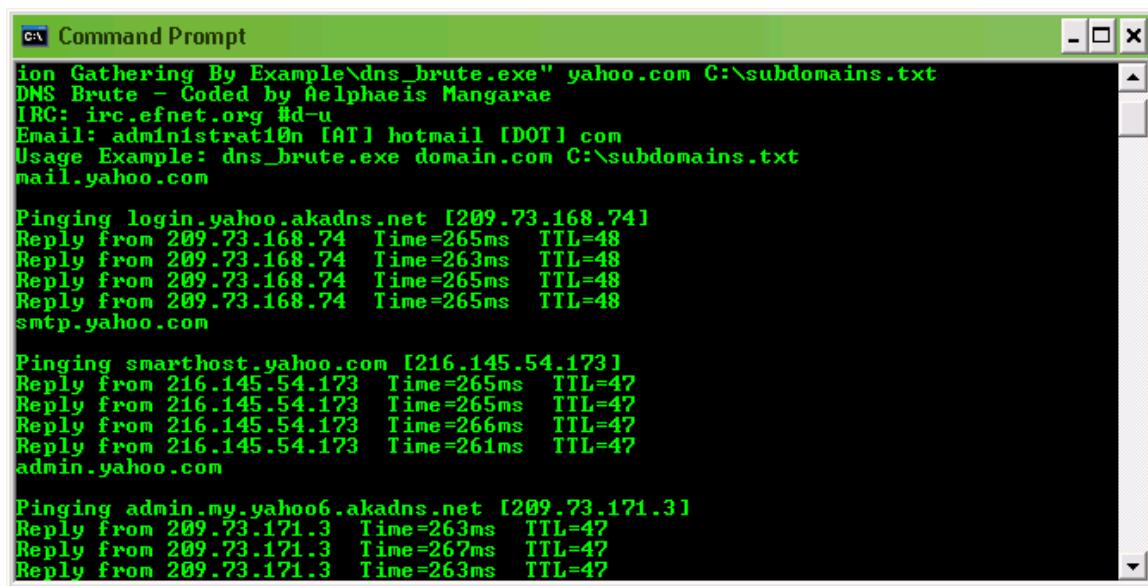
For the purpose of this paper I will just run my program against Yahoo.com



```
C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

E:\Documents and Settings\Chris Morganti.MORGANTI-0LEY09>"C:\My Stuff\My Documents\IT Security\Documents\My White Papers\Uncompleted White Papers\Learn Information Gathering By Example\dns_brute.exe" yahoo.com C:\subdomains.txt
```

This is the result:



```
C:\ Command Prompt
Gathering By Example\dns_brute.exe" yahoo.com C:\subdomains.txt
DNS Brute - Coded by Aelphaeis Mangarae
IRC: irc.efnet.org #d-u
Email: administrati0n [AT] hotmail [DOT] com
Usage Example: dns_brute.exe domain.com C:\subdomains.txt
mail.yahoo.com

Pinging login.yahoo.akadns.net [209.73.168.74]
Reply from 209.73.168.74 Time=265ms TTL=48
Reply from 209.73.168.74 Time=263ms TTL=48
Reply from 209.73.168.74 Time=265ms TTL=48
Reply from 209.73.168.74 Time=265ms TTL=48
smtp.yahoo.com

Pinging smarthost.yahoo.com [216.145.54.173]
Reply from 216.145.54.173 Time=265ms TTL=47
Reply from 216.145.54.173 Time=265ms TTL=47
Reply from 216.145.54.173 Time=266ms TTL=47
Reply from 216.145.54.173 Time=261ms TTL=47
admin.yahoo.com

Pinging admin.my.yahoo6.akadns.net [209.73.171.3]
Reply from 209.73.171.3 Time=263ms TTL=47
Reply from 209.73.171.3 Time=267ms TTL=47
Reply from 209.73.171.3 Time=263ms TTL=47
```

As you can see we have found some useful information for Penetration Testing (no I am not conducting one against Yahoo, I am simply using this as an example.)  
What we have found is the direct DNS' of machines belonging to Yahoo.

**\*The source code to DNS Brute is included with this paper\***

## Performing A Ping Sweep

This is a really basic thing, which you should all know how to do. However since it is part of Information Gathering and being that there is a chance total beginners may read this, I will cover this.

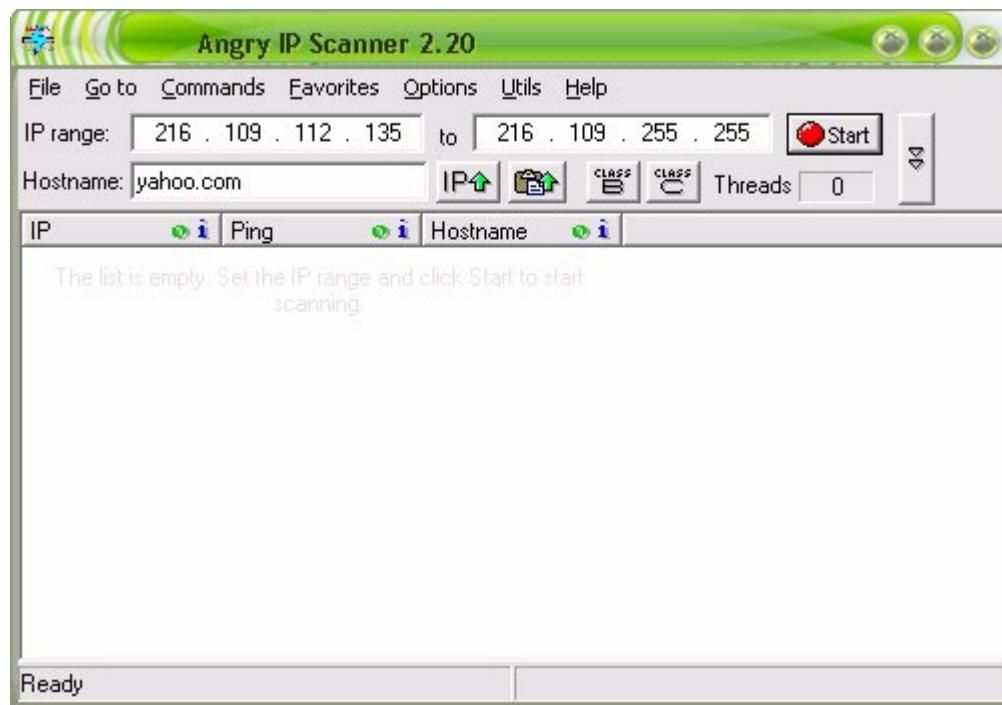
The program we are going to use is **Angry IP Scanner** which can be downloaded from:  
<http://www.angryziber.com/ipscan/>

There are 3 reasons why we are using Angry IP Scanner, the first being it is easy to use, the second being it is a very fast scanner and last of all it has some useful plug-ins for scanning.

Before we begin, for those of you who aren't total beginners (and shouldn't be reading this anyway) I do realize what I am doing is actually more scanning than just doing a normal ping sweep, but why waste a ping sweep? Why not add in something interesting.

The first thing we have to do is get the IP Block/Range, this can usually be retrieved from the Whois, however if it isn't simply estimate an approximate range based upon its IP Address.

Now we fire up Angry IP Scanner.

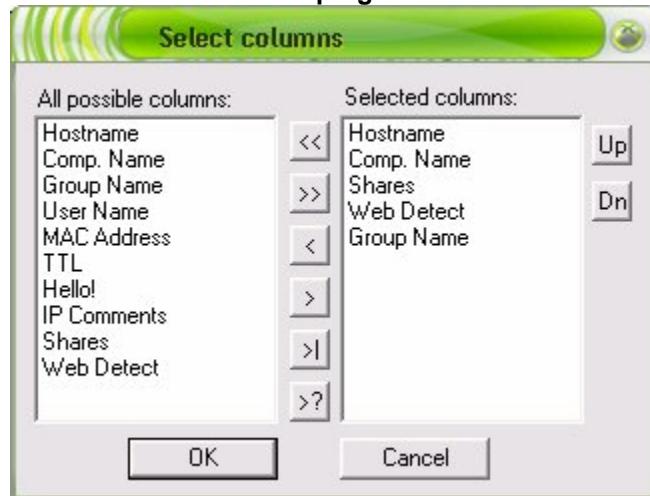


A neat thing about Angry IP Scanner is you can instantly convert a DNS to an IP Address (very handy.)

Now with this I have estimated an approximate IP range. Before I begin the scan, I will use one of Angry IP Scanners **optional plug-ins** which can be downloaded from the website.

If we go into Options -> Select Columns we can chose which plug-ins and information we want to view when doing a scan.

I have chosen to use all plug-ins that I think will show important information.



Now we begin the scan.

Ok now I haven't completed the scan, but I have done enough. A useful thing about Angry IP Scanner is that you can cull all of all the dead hosts so you can have a good look at the live ones.

The screenshot shows the main interface of Angry IP Scanner 2.20. At the top, there's a menu bar with File, Go to, Commands, Favorites, Options, Utils, and Help. Below that is a toolbar with buttons for IP range selection, file operations (Open, Save, etc.), and thread management. The main area is a table displaying scan results. The columns are: IP, Ping, Hostname, Comp. Na..., Shares, Web Detect, and Group Na... . The table lists numerous IP addresses, mostly from the 216.109.112 range, with their corresponding hostnames and other details. Many entries show 'N/A' for various fields, while others show 'UNKNOWN'. The table has scroll bars, indicating it contains many rows of data.

IP	Ping	Hostname	Comp. Na...	Shares	Web Detect	Group Na...
216.109.112...	577 ms	w2.rc.vip.dcn.ya...	N/A	N/A	UNKNOWN	N/A
216.109.112...	639 ms	bs1.ads.vip.dcn...	N/A	N/A	UNKNOWN	N/A
216.109.112...	673 ms	relay1.msg.vip.d...	N/A	N/A	N/A	N/A
216.109.112...	701 ms	tileint1.maps.vip...	N/A	N/A	N/A	N/A
216.109.112...	958 ms	e3-v6-fw.corp.d...	N/A	N/A	UNKNOWN	N/A
216.109.112...	994 ms	ems-db1.cc.corp...	N/A	N/A	N/A	N/A
216.109.112...	1004 ms	ems-db2.cc.corp...	N/A	N/A	UNKNOWN	N/A
216.109.112...	1003 ms	ems-web1.cc.co...	N/A	N/A	UNKNOWN	N/A
216.109.112...	999 ms	ems-app1.cc.cor...	N/A	N/A	N/A	N/A
216.109.112...	1076 ms	ems-app2.cc.cor...	N/A	N/A	UNKNOWN	N/A
216.109.112...	1072 ms	ems-fs1.cc.corp...	N/A	N/A	N/A	N/A
216.109.112...	1215 ms	e3-1v2-second-f...	N/A	N/A	N/A	N/A
216.109.112...	1101 ms	build0.travel.cor...	N/A	N/A	N/A	N/A
216.109.112...	1104 ms	build1.travel.cor...	N/A	N/A	N/A	N/A
216.109.112...	1093 ms	bouncer01.by.c...	N/A	N/A	N/A	N/A
216.109.112...	1124 ms	bouncer01a.by....	N/A	N/A	N/A	N/A
216.109.112...	1123 ms	bouncer01b.by....	N/A	N/A	N/A	N/A
216.109.112...	1160 ms	bouncer01c.by....	N/A	N/A	UNKNOWN	N/A
216.109.112...	1170 ms	login4.corp.dcn...	N/A	N/A	N/A	N/A
216.109.112...	1203 ms	socks.corp.dcn...	N/A	N/A	UNKNOWN	N/A
216.109.112...	1245 ms	nc1.bcp.corp.dc...	N/A	N/A	N/A	N/A
216.109.112...	0ms ...	...L...-L...-L...-	N/A	N/A	UNKNOWN	N/A

What have we been able to gather from this? Well first of all we have some host names. The second thing I have learnt about Yahoo is they hide the identity of their web servers. Now this is a good security practice, Yahoo have been hacked before, and they don't want website defacers scanning their IP range and looking for outdated web servers.

## Identifying Firewalls/Routers

It is possible and quite a simple task to Identify remote routers, firewalls and other devices. This can be done simply by using Trace Route.

Now both Windows and Linux operating systems have command line tools that allow us to accomplish this.

On Windows it is “tracert”, and on Linux “traceroute”.

Because I am using Windows at the moment I will demonstrate the use of tracert.

Tracing route to yahoo.com [66.94.234.13]  
over a maximum of 30 hops:

```
1  80 ms  69 ms  77 ms  10.0.0.2
2  81 ms  100 ms 123 ms  ains-202-126-96-250.ains.net.au [202.126.96.250]
3  71 ms  71 ms  71 ms  202.147.100.2
4  74 ms  73 ms  77 ms  203.82.183.157
5  75 ms  71 ms  75 ms  203.82.183.153
6  74 ms  77 ms  73 ms  326.ge-0-0-GW4.MEL1.ALTER.NET [221.133.202.9]
7  80 ms  75 ms  89 ms  424.AT-6-0-0.XR1.MEL1.ALTER.NET [210.80.33.161]
8  82 ms  79 ms  81 ms  so-6-1-0.XR2.MEL1.ALTER.NET [210.80.33.26]
9  106 ms 103 ms  97 ms  so-0-1-0.XT2.SYD4.ALTER.NET [210.80.33.9]
10 182 ms  92 ms  125 ms  so-5-0-0.XT1.SYD4.ALTER.NET [210.80.33.213]
11 249 ms  252 ms  249 ms  0.so-4-2-0.IR1.SAC2.Alter.Net [210.80.50.141]
12 272 ms  243 ms  274 ms  POS3-0.IR1.SAC1.ALTER.NET [137.39.31.194]
13 291 ms  337 ms  251 ms  0.so-0-0-TL1.SAC1.ALTER.NET [152.63.0.114]
14 247 ms  247 ms  241 ms  0.so-5-0-0.XL1.SCL2.ALTER.NET [152.63.57.41]
15 254 ms  253 ms  253 ms  0.so-6-0-0.BR1.SCL2.ALTER.NET [152.63.57.49]
16 250 ms  249 ms  256 ms  204.255.173.42
17 277 ms  273 ms  247 ms  so-1-2-0.bbr1.SanJose1.Level3.net [209.244.3.137]
18 243 ms  247 ms  255 ms  ae-13-55.car3.SanJose1.Level3.net [4.68.123.141]
19 248 ms  251 ms  249 ms  4.71.112.14
20 282 ms  274 ms  253 ms  ge-3-0-0-p271.msr2.scd.yahoo.com [216.115.106.191]
21 248 ms  269 ms  251 ms  ten-2-3-bas2.scd.yahoo.com [66.218.82.223]
22 248 ms  267 ms  247 ms  w2.rc.vip.scd.yahoo.com [66.94.234.13]
```

Trace complete.

As you can see the first hop is my router, the second is my ISP.

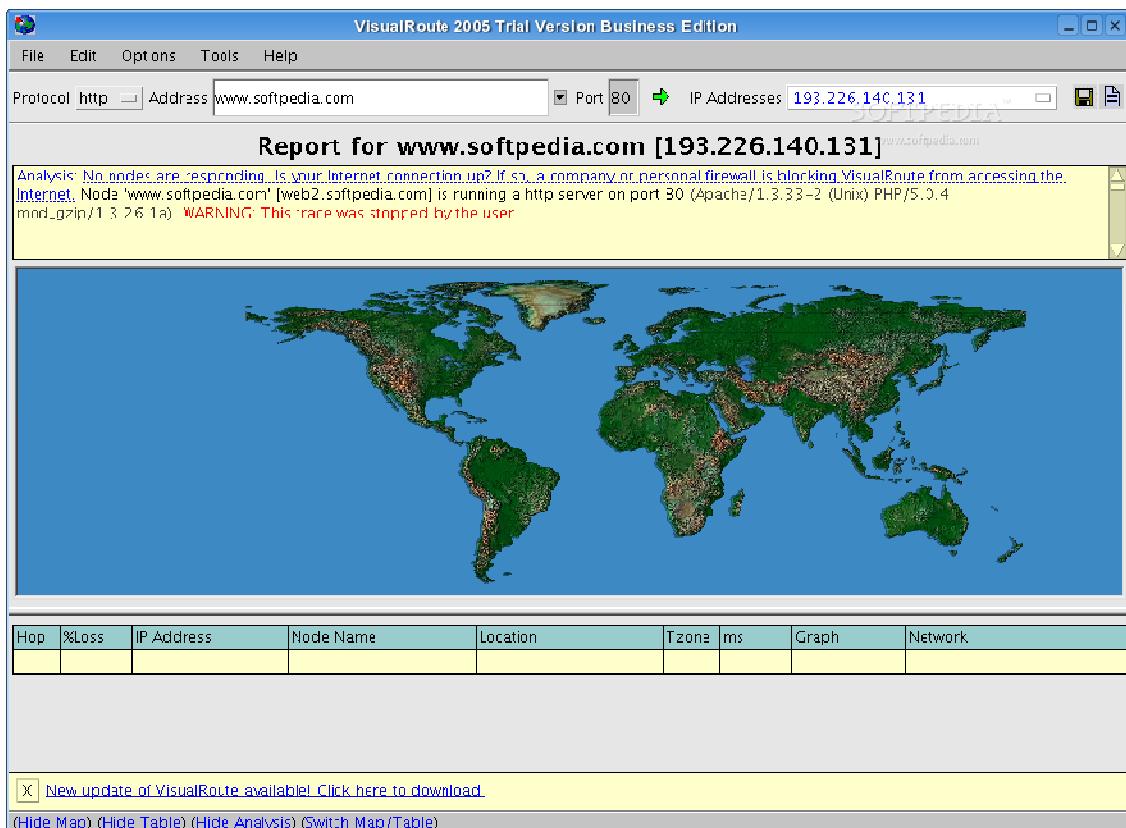
At about the 19<sup>th</sup> hop the trace is approaching some of the Routers (or other devices) used by Yahoo.

**In a penetration testing these devices are things you are going to want to focus on (among other things of course.)**

For those of you who do not like using a Command Line there is a program available called **Visual Route** - <http://www.visualroute.com/>

Visual Route has a graphical user interface and actually has a world map you can visually see where each hop is on the trace.

Here is a screenshot of Visual Route:

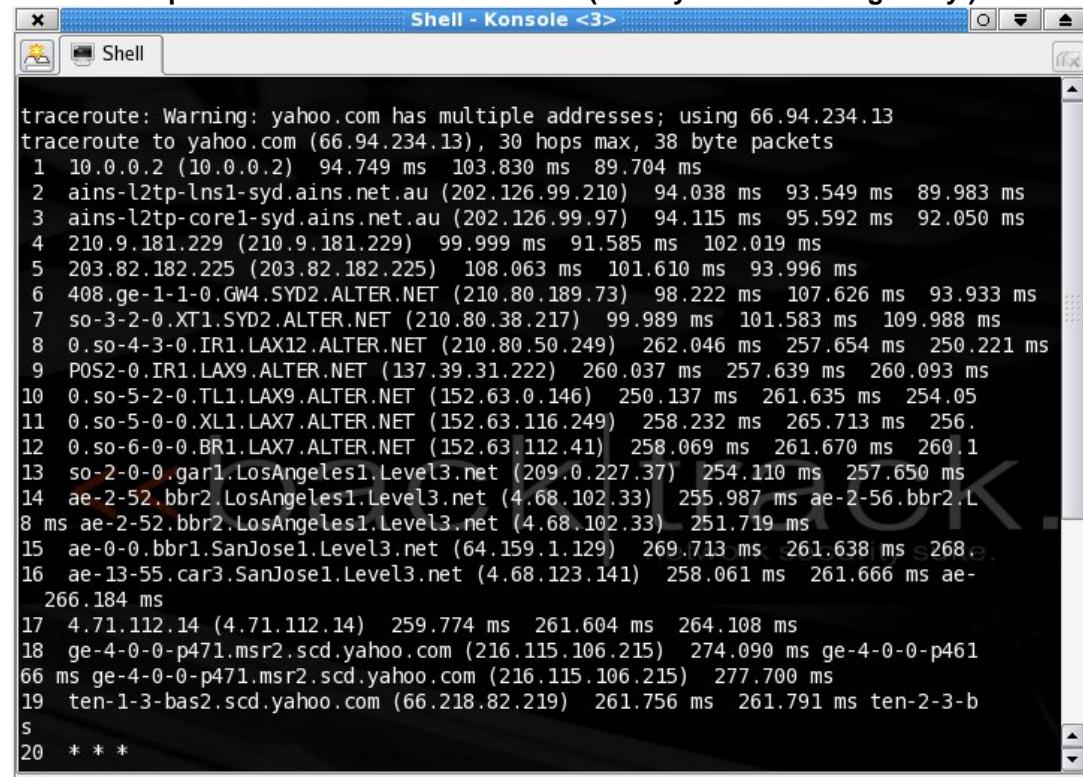


### One last thing about Trace Route.

You may notice when using the command line version that some hosts do not respond, yet the host afterwards does.

This means that the host that doesn't respond isn't responding to ICMP packets, yet allows ICMP packets to travel through. The command line version of Trace Route in both Windows and Linux uses ICMP packets to do the trace.

The Linux equivalent of Tracert is Traceroute (exactly the same thing really.)



```
traceroute: Warning: yahoo.com has multiple addresses; using 66.94.234.13
traceroute to yahoo.com (66.94.234.13), 30 hops max, 38 byte packets
 1  10.0.0.2 (10.0.0.2)  94.749 ms  103.830 ms  89.704 ms
 2  ains-l2tp-lns1-syd.ains.net.au (202.126.99.210)  94.038 ms  93.549 ms  89.983 ms
 3  ains-l2tp-core1-syd.ains.net.au (202.126.99.97)  94.115 ms  95.592 ms  92.050 ms
 4  210.9.181.229 (210.9.181.229)  99.999 ms  91.585 ms  102.019 ms
 5  203.82.182.225 (203.82.182.225)  108.063 ms  101.610 ms  93.996 ms
 6  408.ge-1-1-0.GW4.SYD2.ALTER.NET (210.80.189.73)  98.222 ms  107.626 ms  93.933 ms
 7  so-3-2-0.XT1.SYD2.ALTER.NET (210.80.38.217)  99.989 ms  101.583 ms  109.988 ms
 8  0.so-4-3-0.IR1.LAX12.ALTER.NET (210.80.50.249)  262.046 ms  257.654 ms  250.221 ms
 9  POS2-0.IR1.LAX9.ALTER.NET (137.39.31.222)  260.037 ms  257.639 ms  260.093 ms
10  0.so-5-2-0.TL1.LAX9.ALTER.NET (152.63.0.146)  250.137 ms  261.635 ms  254.05
11  0.so-5-0-0.XL1.LAX7.ALTER.NET (152.63.116.249)  258.232 ms  265.713 ms  256.
12  0.so-6-0-0.BR1.LAX7.ALTER.NET (152.63.112.41)  258.069 ms  261.670 ms  260.1
13  so-2-0-0.gar1.LosAngeles1.Level3.net (209.0.227.37)  254.110 ms  257.650 ms
14  ae-2-52.bbr2.LosAngeles1.Level3.net (4.68.102.33)  255.987 ms ae-2-56.bbr2.L
8 ms ae-2-52.bbr2.LosAngeles1.Level3.net (4.68.102.33)  251.719 ms
15  ae-0-0.bbr1.SanJose1.Level3.net (64.159.1.129)  269.713 ms  261.638 ms  268.e.
16  ae-13-55.car3.SanJose1.Level3.net (4.68.123.141)  258.061 ms  261.666 ms ae-
266.184 ms
17  4.71.112.14 (4.71.112.14)  259.774 ms  261.604 ms  264.108 ms
18  ge-4-0-0-p471.msr2.scd.yahoo.com (216.115.106.215)  274.090 ms ge-4-0-0-p461
66 ms ge-4-0-0-p471.msr2.scd.yahoo.com (216.115.106.215)  277.700 ms
19  ten-1-3-bas2.scd.yahoo.com (66.218.82.219)  261.756 ms  261.791 ms ten-2-3-b
s
20  * * *
```

Usage: traceroute host.com

## Gathering Information From Emails

Gathering Information from Emails you say? Yes, some very handy information can be gathered from emails.

You can obtain information simply by sending an email and then receiving one.  
Useful information is contained in the email headers.

```
MIME-Version: 1.0
Received: from mail.networksolutionsemail.com ([205.178.146.55]) by bay0-mc3-
f10.bay0.hotmail.com with Microsoft SMTPSVC(6.0.3790.211); Fri, 30 Dec 2005 14:27:13 -0800
Received: (qmail 21220 invoked from network); 30 Dec 2005 22:26:56 -0000
Received: from unknown (HELO rsa33) (67.49.231.86) by 10.49.34.115 with SMTP; 30 Dec 2005
22:26:56 -0000
X-Message-Info: JGTYoYF78jHECf9u/HR9ZmEHdSU/U1KwbJMtUcimNDw=
Organization: ksd,inc
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2800.1437
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1441
Return-Path: rsa@ksdinc.net
X-OriginalArrivalTime: 30 Dec 2005 22:27:13.0637 (UTC) FILETIME=[2EAFE950:01C60D90]
```

From this we can gather numerous pieces of information such as:

**SMTP Server:** mail.networksolutionsemail.com  
**SMTP Software:** Microsoft SMTPSVC(6.0.3790.211)  
**Time/Date Email Received:** 30 Dec 2005 22:26:56  
**IP Address Of Sender:** 67.49.231.86  
**Email Software:** Microsoft Outlook Express 6.00.2800.1437  
**From Email Address:** rsa@ksdinc.net

So we have gathered some useful information. To get more information we can do a Whois on some of the IP Addresses and DNS' above.

Have a look over the email headers and then have a look at the information I have listed out so you can see where I got it all from.

By default Hotmail (What Email provider I use) does not allow you to view all the headers of an email. To change this go to **Options -> Mail Display Settings, then turn Message headers to Advanced.**

Now for those of you who are using Microsoft Outlook this may help you:

<http://office.microsoft.com/en-us/assistance/ha010937071033.aspx>

## Obtaining Information With Scripts

Using PHP and Javascript we can gather information on a target host. Now as most of you know this can only be done by getting them to view HTML (whether it be a website or HTML email.) Here is a link which shows the sort of information which can be gathered using a script:

<http://www.irongeek.com/browserinfo.php>

Obviously we can't personally use the link to gather information. However we can use other scripts to. I recommend:

<http://statcounter.com>

You can get a piece of Javascript code that when loaded on a remote machines can gather information on the person(s) loading the page.

I have one on my website <http://911physics.co.nr>

Although I mainly use Stat Counter to count how many unique visits my website gets I can also have a look at information relating to visitors that come to my website.

**One thing I usually notice is that after a vulnerability is discovered in Firefox it usually takes people literally weeks to upgrade their browser! (To the latest version.)**

Using Stat Counter is easy enough, it is just a matter of making an account and then getting the code to add into your webpage (or other HTML page.)

This is an example of the information that can be gathered:

VISITOR ANALYSIS	
Referring Link	<a href="http://911physics.co.nr/">http://911physics.co.nr/</a>
Host Name	BEWC315-BC-2B.belvoir.army.mil
IP Address	128.190.62.54
Country	United States
Region	Virginia
City	Ft. Belvoir
ISP	Directorate Of Automation Services
Returning Visits	2
Visit Length	1 hour 3 mins 26 secs
VISITOR SYSTEM SPECS	
Browser	MSIE 6.0
Operating System	Windows 2003
Resolution	1024x768
Javascript	Enabled

We have successfully gathered details on:

**Operating System**

**Web Browser**

**Javascript Enabled/Disabled**

As well as a couple of other potentially useful pieces of information.

## About The Author

Aelphaeis Mangarae is an Administrator at Igniteds Security Forums – <http://Igniteds.net> as well as at **Zone-H.org**

I have authored several other White Papers which include **Hardening Windows NT, XSS Attacks FAQ & Steganography FAQ.**

I have also recently become an Administrator at **SecurZone.Org**.  
(SecurZone.Org will be coming back soon!)

I am also a student member of the Scholars for 9/11 Truth – <http://st911.org>

**IRC:** irc.efnet.org #d-u

**Email:** adm1n1strat10n [AT] hotmail [DOT] com

**MSN Messenger:** adm1n1strat10n [AT] hotmail [DOT] com

**Xbox Live Gamer Tag:** Aelphaeis

## Greetz To

htek, HackJoeSite, FRSilent, Read101, tomchu, nic`, BSoD, r0rkty, Nitrous, SyS64738, Trash-80, morning\_wood, Astharot, Fauley, Furax, PsAuX, SecurityWireless, SysSpider, Siegfried, fritz, darkt3ch, Predator/ill skillz, Alchemist, BioHunter, Digerati, digital-flow, butthead, spiderlance, FishNET, W--, nrs, IBMWarpst, Nixus, varu, z16bitseg, PTP, felosi, Mega-biT<sub>e</sub>, wicked/aera, Palmeiro, Kadafiu, sNKenjoi, tgo, melkor, mu-tiger, royal, Wex, ksv, GoTiT4FrE, CKD, Dr4g, Coldfisher, snx, skiddielet, ProwL, drygol, kon, Iadnah, EwenG, belgther, sarkar112, str0ke and Kenny & Blake from GSO.

sarkar112 – Thanks for pointing out that little grammar error in the draft paper.

htek, tgo, wicked – Thanks for all the help with stuff unrelated to this paper. I really appreciate it.

r0rkty – Looking forward to running SecurZone with you!

snx – Thanks for the SecurZone banner.

**h4cky0u – How long are you going to ignore me for?**