Digital Reconnaissance

Information Gathering for a Security Review

Jake Meredith
Security Engineer
iSEC Partners

Agenda

- Passive Information Gathering
- Tools!
- Active Information Gathering
- More Tools!!

Security Review

- What is it?
- Why would you need one?
- Where can you get one? (hint: iSEC)

Legality

- Public sources of information are technically legal, what you do with those sources may not be.
- NEVER access data you are not permitted to access, scanning, pen testing, etc.

Information Gathering

- Find as much information as you can about a target
  - Find weaknesses
  - Prep for Social Engineering attacks
- Use 3rd party resources for finding information
  - Google, Facebook, Twitter, etc.
- Use Company’s own resources
  - Website - email addresses, company structure
  - Physical – garbage, physical security
  - Network infrastructure – public services, open ports, etc.

Operating System

- Backtrack
  - Penetration Testing and Security Auditing Linux Distribution
  - Lots of built-in tools
  - Nothing you can’t install on other distros but packaged together nicely
  - www.**backtrack**-linux.org

Passive vs Active

- Passive
  - Don’t interact directly with company
  - Stealthier with respect to target company
  - Usually not as much data
- Active
  - Interact directly with company
  - Harder to be stealthy (TOR, web proxy, etc)
  - Usually much more data

Passive Reconnaissance

- Art of gathering information from publicly available sources
- Companies display a lot of useful information on websites and social networks
- Employees post even more interesting things in forums, social networks, and blogs
- Many companies exist that monitor and cache the web and provide data for public consumption

The Googles

- Search operators:
  - site: isecpartners.com
  - inurl: isecpartners
  - filetype: .pdf
  - Wildcard (*)
- Google Hacking Database
  - Less targeted usually
  - Can find some interesting searches to try for your target
  - “login: *” “password= *” filetype:xls

Alternate Search Engines

- Bing!
  - Search by IP
    - ip:
- Gigablast
  - Returns *different* results
    - http://www.gigablast.com/search?k1h=999341&q=isecpartners.com
- Wayback Machine
  - Check previous versions of website to reveal things they may have removed

theHarvester

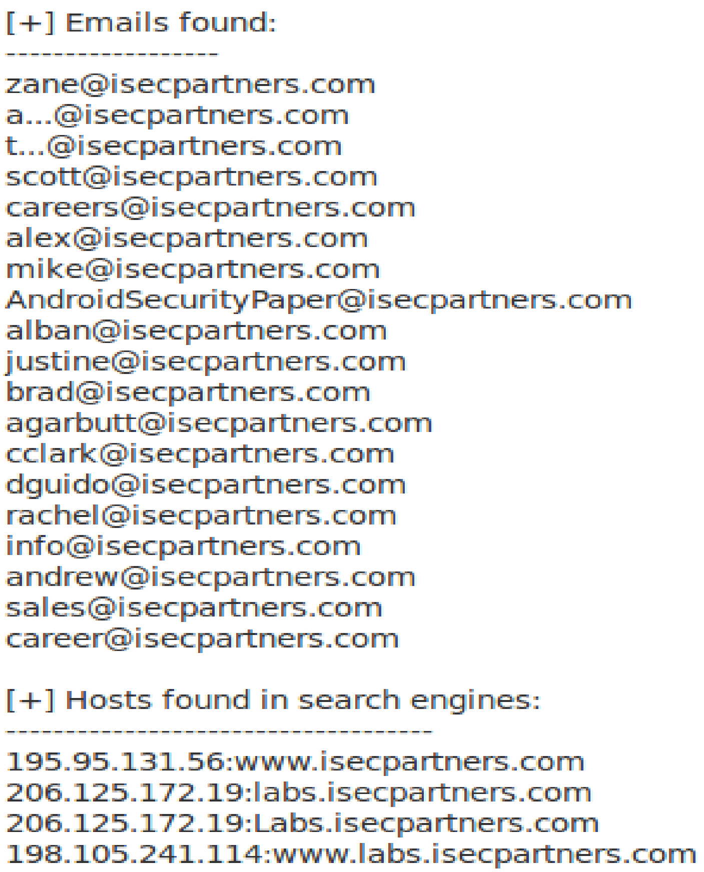
- /pentest/enumeration/theharvester
- Uses search engines to mine data
- Can specify search engines

```
./theHarvester.py -d isecpartners.com -b google
```

```
./theHarvester.py -d nccgroup -b bing
```

theHarvester Output

./theHarvester.py -d isecpartners.com -l 200 -b google



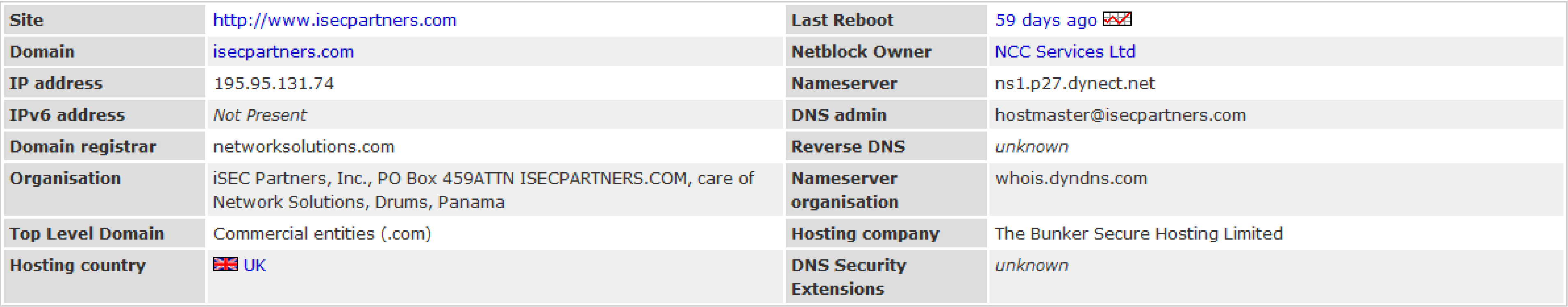
```
[+] Emails found:
------------------
zane@isecpartners.com
a...@isecpartners.com
t...@isecpartners.com
scott@isecpartners.com
careers@isecpartners.com
alex@isecpartners.com
mike@isecpartners.com
AndroidSecurityPaper@isecpartners.com
alban@isecpartners.com
justine@isecpartners.com
brad@isecpartners.com
agarbutt@isecpartners.com
cclark@isecpartners.com
dguido@isecpartners.com
rachel@isecpartners.com
info@isecpartners.com
andrew@isecpartners.com
sales@isecpartners.com
career@isecpartners.com

[+] Hosts found in search engines:
------------------------------------
195.95.131.56:www.isecpartners.com
206.125.172.19:labs.isecpartners.com
206.125.172.19:Labs.isecpartners.com
198.105.241.114:www.labs.isecpartners.com
```

Netcraft

- Internet monitoring company
- Has large amounts of data about public facing websites, provides data in searchable format
- Monitors uptime and server OS

Netcraft Output

- searchdns.netcraft.com



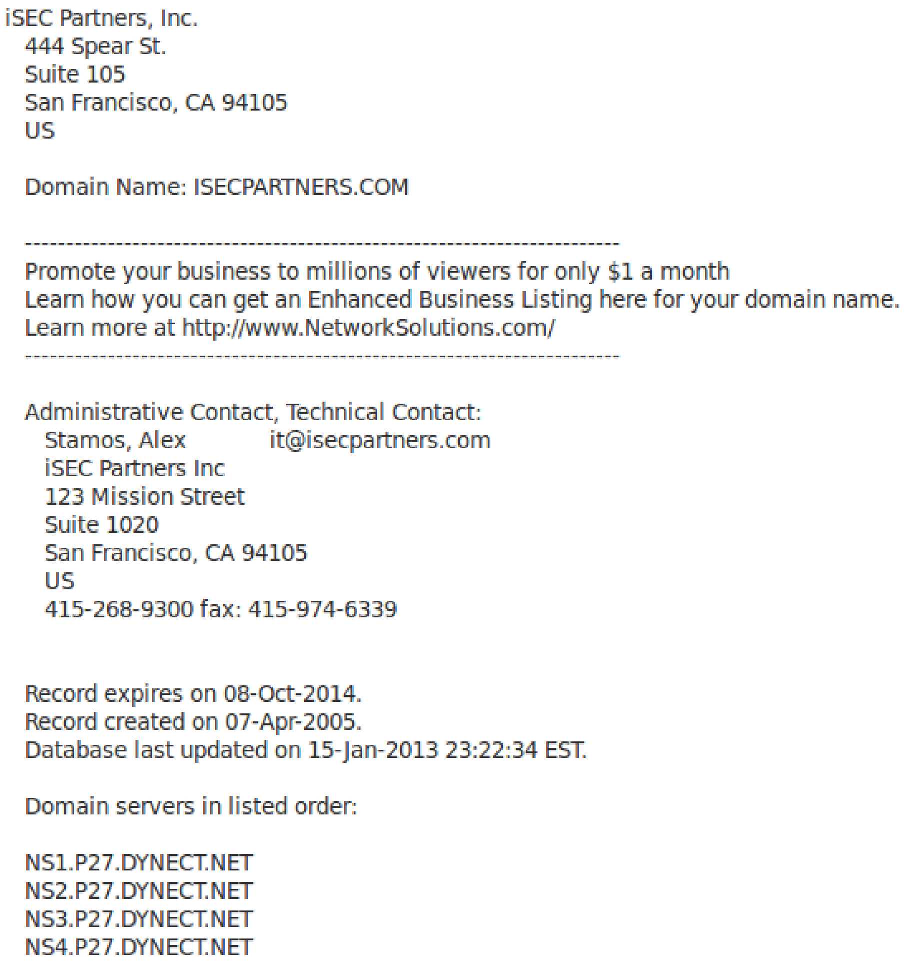
Site	http://www.isecpartners.com	**Last Reboot**	59 days ago
Domain	isecpartners.com	**Netblock Owner**	NCC Services Ltd
IP address	195.95.131.74	**Nameserver**	ns1.p27.dynect.net
IPv6 address	*Not Present*	**DNS admin**	hostmaster@isecpartners.com
Domain registrar	networksolutions.com	**Reverse DNS**	*unknown*
Organisation	iSEC Partners, Inc., PO Box 459ATTN ISECPARTNERS.COM, care of Network Solutions, Drums, Panama	**Nameserver organisation**	whois.dyndns.com
Top Level Domain	Commercial entities (.com)	**Hosting company**	The Bunker Secure Hosting Limited
Hosting country	🇬🇧 UK	**DNS Security Extensions**	*unknown*

Whois

- Addresses, contact names, email addresses, domain servers
- Alternates: whois.domaintools.com, ripe.net, whois.sc

```
$whois isecpartners.com
```

Whois Output



```
iSEC Partners, Inc.
   444 Spear St.
   Suite 105
   San Francisco, CA 94105
   US

   Domain Name: ISECPARTNERS.COM

   ------------------------------------------------------------------------
   Promote your business to millions of viewers for only $1 a month
   Learn how you can get an Enhanced Business Listing here for your domain name.
   Learn more at http://www.NetworkSolutions.com/
   ------------------------------------------------------------------------

   Administrative Contact, Technical Contact:
      Stamos, Alex            it@isecpartners.com
      iSEC Partners Inc
      123 Mission Street
      Suite 1020
      San Francisco, CA 94105
      US
      415-268-9300 fax: 415-974-6339


   Record expires on 08-Oct-2014.
   Record created on 07-Apr-2005.
   Database last updated on 15-Jan-2013 23:22:34 EST.

   Domain servers in listed order:

   NS1.P27.DYNECT.NET
   NS2.P27.DYNECT.NET
   NS3.P27.DYNECT.NET
   NS4.P27.DYNECT.NET
```

Social Media

- Facebook
  - Usually find a list of employees
  - Times of events, perhaps letting you know when most employees will be out of the office
- LinkedIn
  - List of employees and considerable data about them
  - Check employees skill sets for idea about technology they use

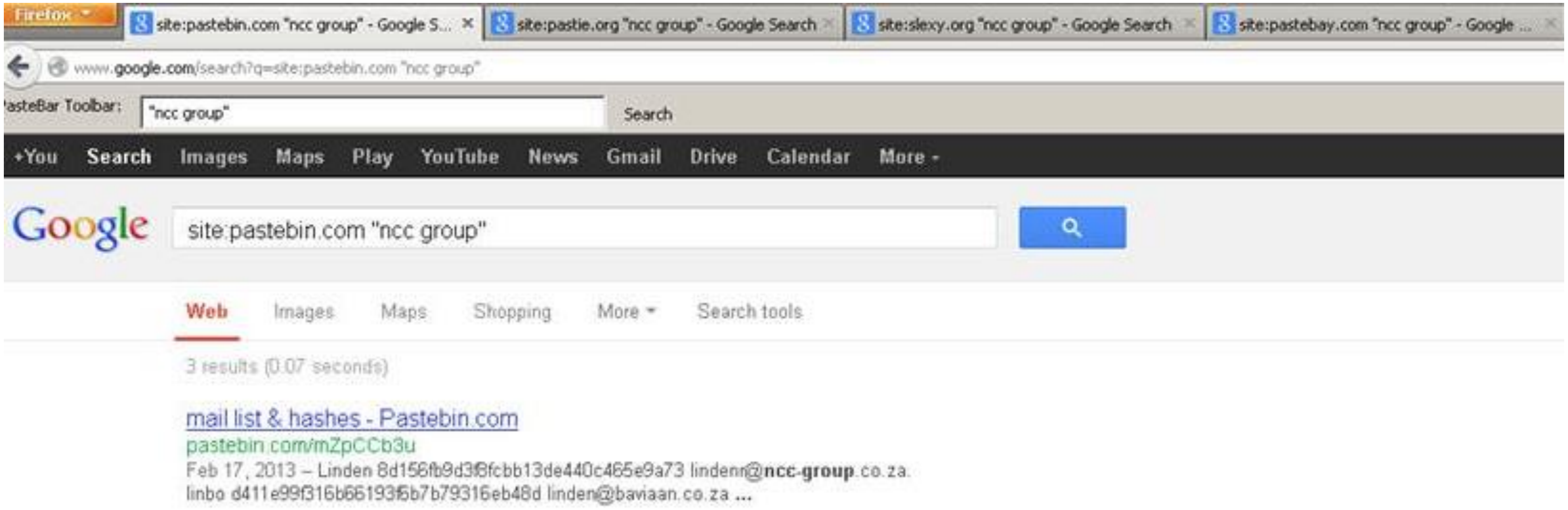
Twitter

- Gold mine for data
- Public APIs –
  - Public -https://dev.twitter.com/docs/streaming-apis/streams/public
  - User - https://dev.twitter.com/docs/streaming-apis/streams/user
  - Site - https://dev.twitter.com/docs/streaming-apis/streams/site
- Many tools are debuting:
  - Twitter bot that searches for phone numbers and addresses
  - Twitter scraper – finds data on topics, people, companies that people are posting about
  - Check the people following a company, lots of employees, you can see what they are posting, information disclosure

Password Dump Sites

- Malicious attackers post data about information disclosure on these dump sites including usernames, passwords, email addresses, emails, etc.
- Pastebin, Paste2, Twitter bots that follow dump sites
- USE GOOGLE:
  - site:pastebin.com “isecpartners”

Pastebin example



Firefox
site:pastebin.com "ncc group" - Google S...
site:pastie.org "ncc group" - Google Search
site:slexy.org "ncc group" - Google Search
site:pastebay.com "ncc group" - Google ...
www.google.com/search?q=site:pastebin.com "ncc group"
PasteBar Toolbar:
Search
+You
Search
Images
Maps
Play
YouTube
News
Gmail
Drive
Calendar
More
Google
Web
Images
Maps
Shopping
More
Search tools

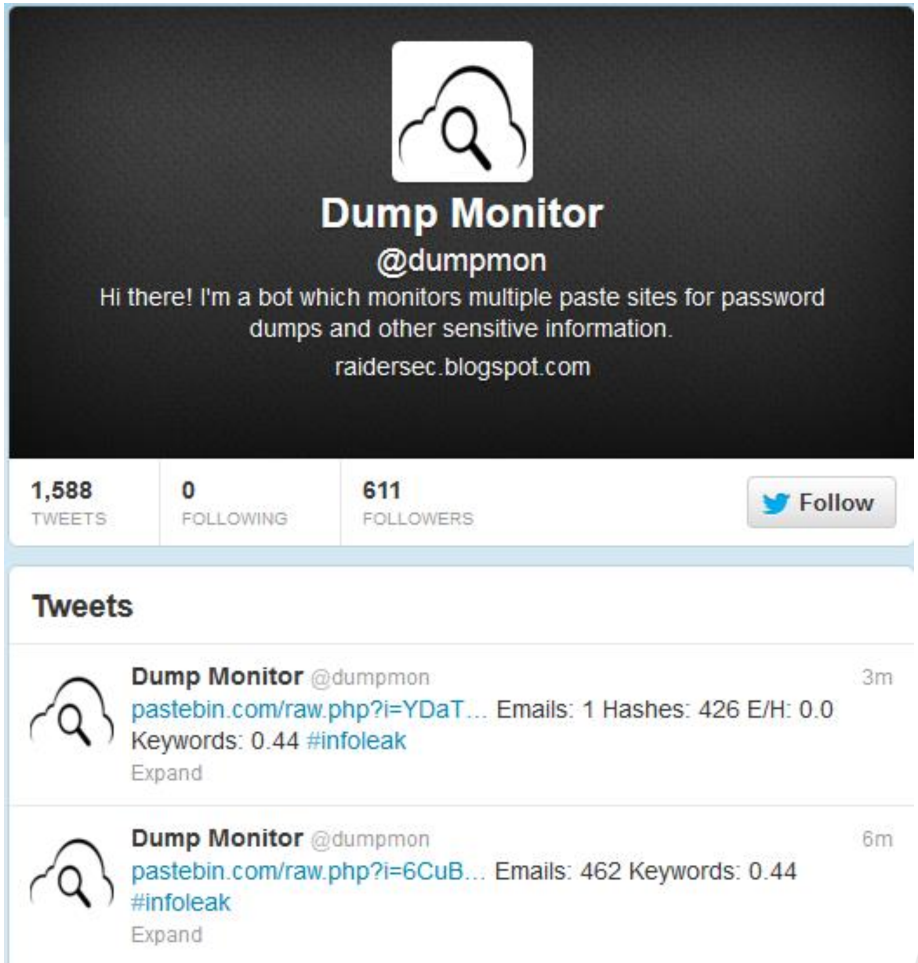
PasteBar Toolbar: "ncc group"

site:pastebin.com "ncc group"

3 results (0.07 seconds)

mail list & hashes - Pastebin.com
pastebin.com/mZpCCb3u
Feb 17, 2013 – Linden 8d156fb9d3f8fcbb13de440c465e9a73 lindenn@**ncc-group**.co.za. linbo d411e99f316b66193f5b7b79316eb48d linden@baviaan.co.za ...

Twitter bot for dump sites



Dump Monitor

@dumpmon

Hi there! I'm a bot which monitors multiple paste sites for password dumps and other sensitive information.

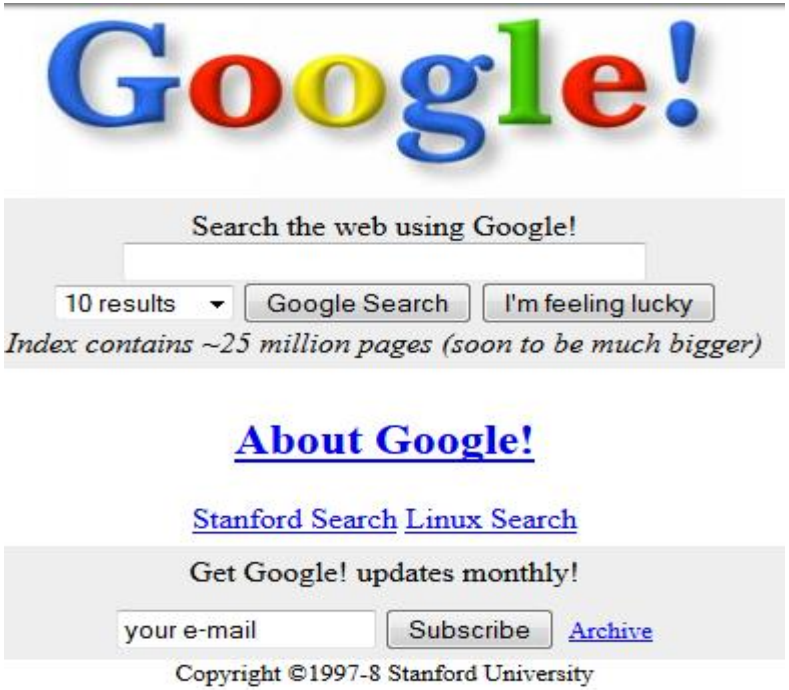
raidersec.blogspot.com

Dump Monitor @dumpmon 3m
pastebin.com/raw.php?i=YDaT... Emails: 1 Hashes: 426 E/H: 0.0 Keywords: 0.44 #infoleak
Expand

Dump Monitor @dumpmon 6m
pastebin.com/raw.php?i=6CuB... Emails: 462 Keywords: 0.44 #infoleak
Expand

Wayback Machine

- http://archive.org/web/web.php
- Check for previous versions of website, perhaps there was more information disclosed in the past
- Or just make fun of really old versions of websites



Index contains ~25 million pages (soon to be much bigger)

Get Google! updates monthly!

Copyright ©1997-8 Stanford University

Attack Vectors with this Data

- Phishing
  - “Hello Jim, IT has a new Thingamabob for you to download. Just click HERE!!!!!”
- Social Engineering
  - “Hello this is Jim from Corporate IT. We are having a problem with our federation access on ServerA and need a new access account. Can you reset my account with a password of ‘password1’ so I can test something? They are really on my ass right now, I appreciate it”
- Blackmail
  - “We have a list of all your passwords. Pay us or we go public”

Active Recon

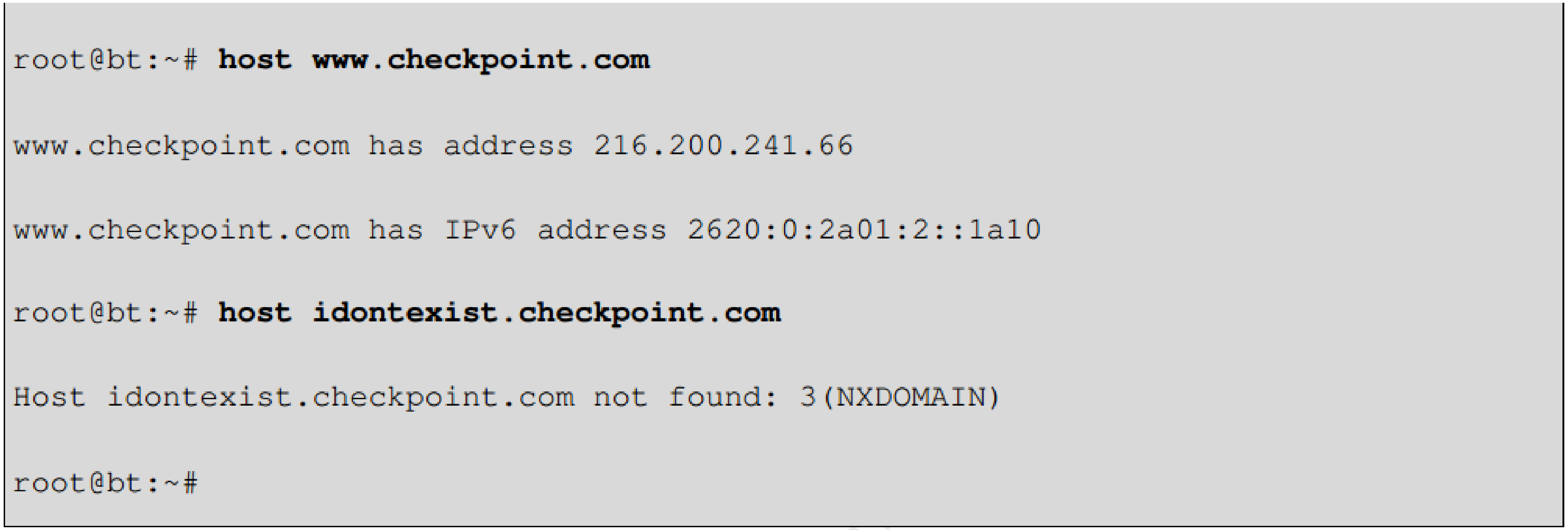
- Directly interact with the target's resources
- DNS servers
- Web servers
- Physical locations
- Scanning public and internal IP range
  - SMTP, SNMP

DNS

- Domain Name System
  - Translates names to IP addresses
  - Can offer information such as server names and server functions.

host

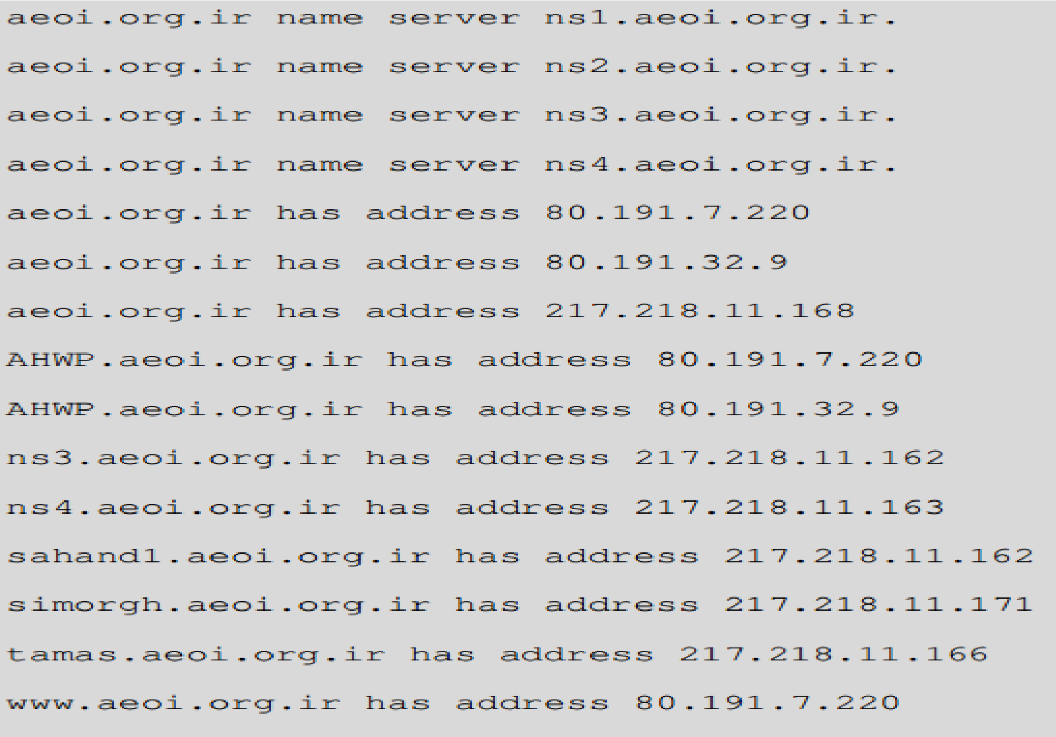
- Check a hostname for validity and return with IP address or the opposite



```
root@bt:~# host www.checkpoint.com

www.checkpoint.com has address 216.200.241.66

www.checkpoint.com has IPv6 address 2620:0:2a01:2::1a10

root@bt:~# host idontexist.checkpoint.com

Host idontexist.checkpoint.com not found: 3(NXDOMAIN)

root@bt:~#
```

host – Zone Transfer

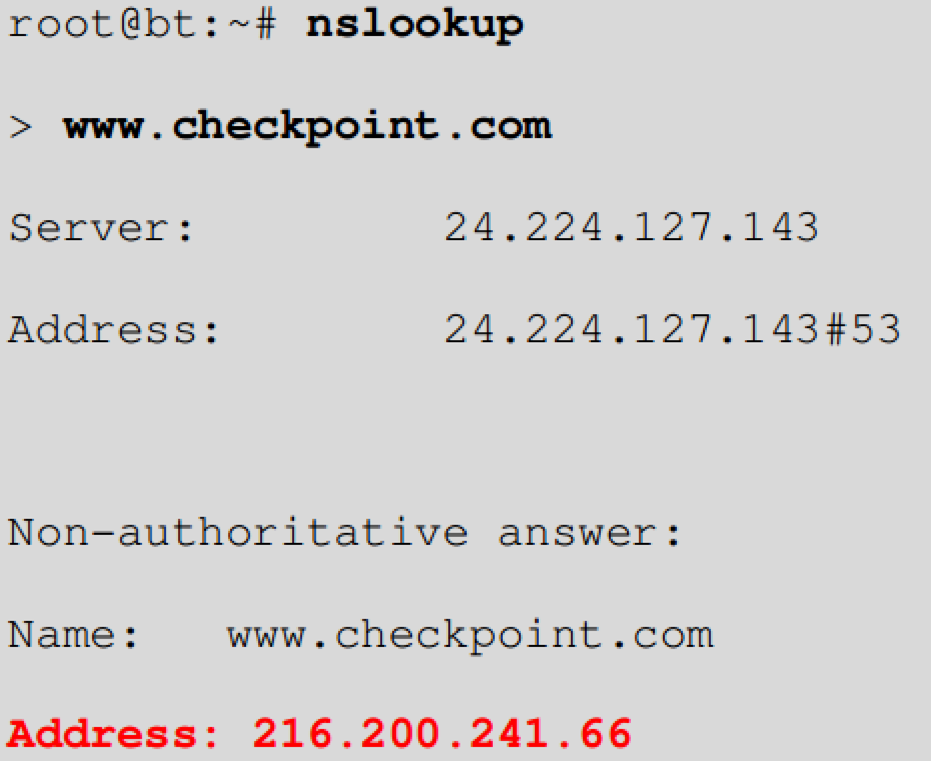
- Zone Transfer – transferring the DNS records off of a DNS server (possibly illegal to do without permission)
- host –l ns1.aeoi.org.ir



```
aeoi.org.ir name server ns1.aeoi.org.ir.
aeoi.org.ir name server ns2.aeoi.org.ir.
aeoi.org.ir name server ns3.aeoi.org.ir.
aeoi.org.ir name server ns4.aeoi.org.ir.
aeoi.org.ir has address 80.191.7.220
aeoi.org.ir has address 80.191.32.9
aeoi.org.ir has address 217.218.11.168
AHWP.aeoi.org.ir has address 80.191.7.220
AHWP.aeoi.org.ir has address 80.191.32.9
ns3.aeoi.org.ir has address 217.218.11.162
ns4.aeoi.org.ir has address 217.218.11.163
sahand1.aeoi.org.ir has address 217.218.11.162
simorgh.aeoi.org.ir has address 217.218.11.171
tamas.aeoi.org.ir has address 217.218.11.166
www.aeoi.org.ir has address 80.191.7.220
```

nslookup

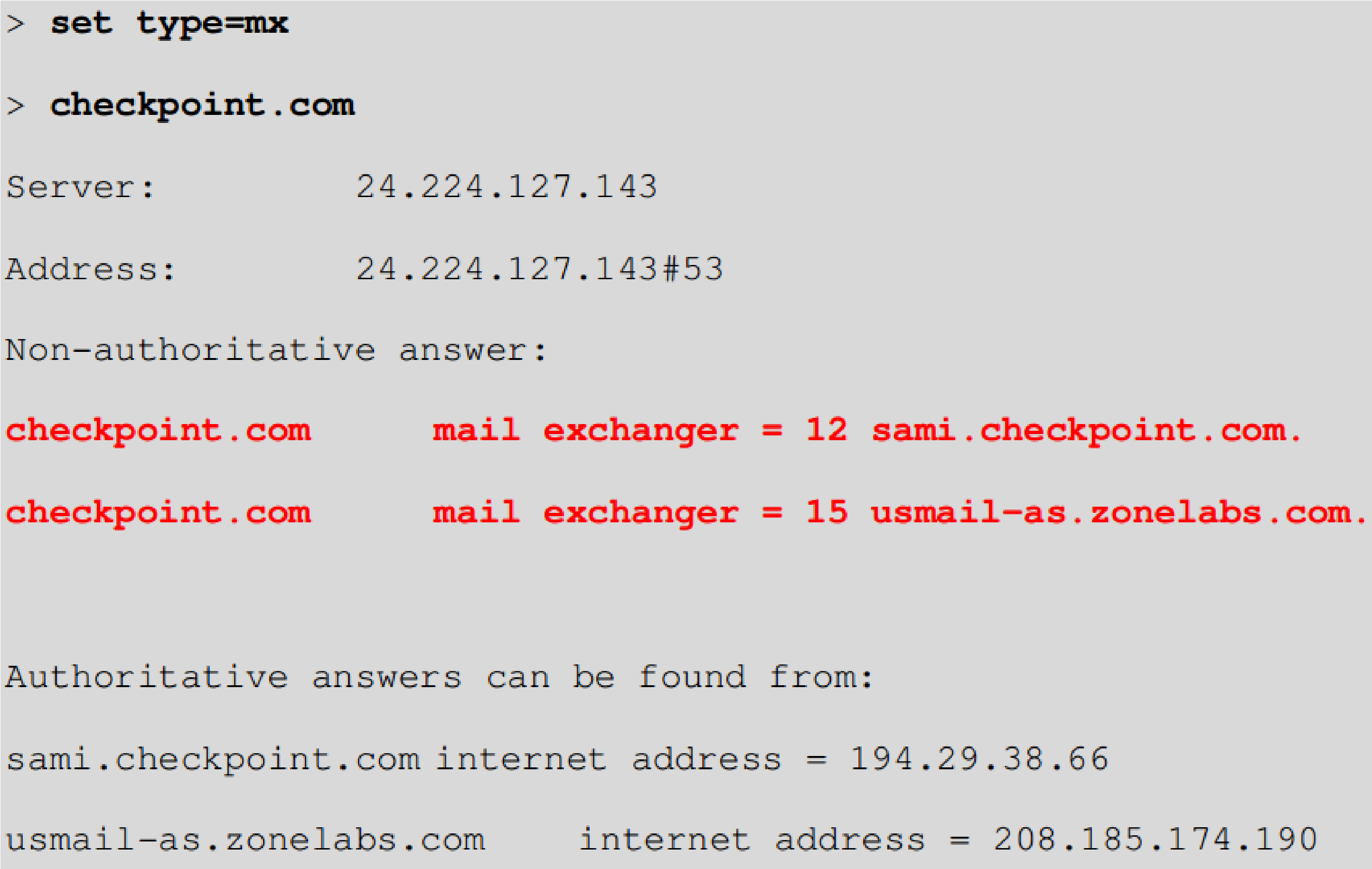
- Forwards DNS requests to your DNS server and asks it to resolve a particular host name



```
root@bt:~# nslookup

> www.checkpoint.com

Server:          24.224.127.143

Address:         24.224.127.143#53



Non-authoritative answer:

Name:    www.checkpoint.com

Address: 216.200.241.66
```

nslookup options

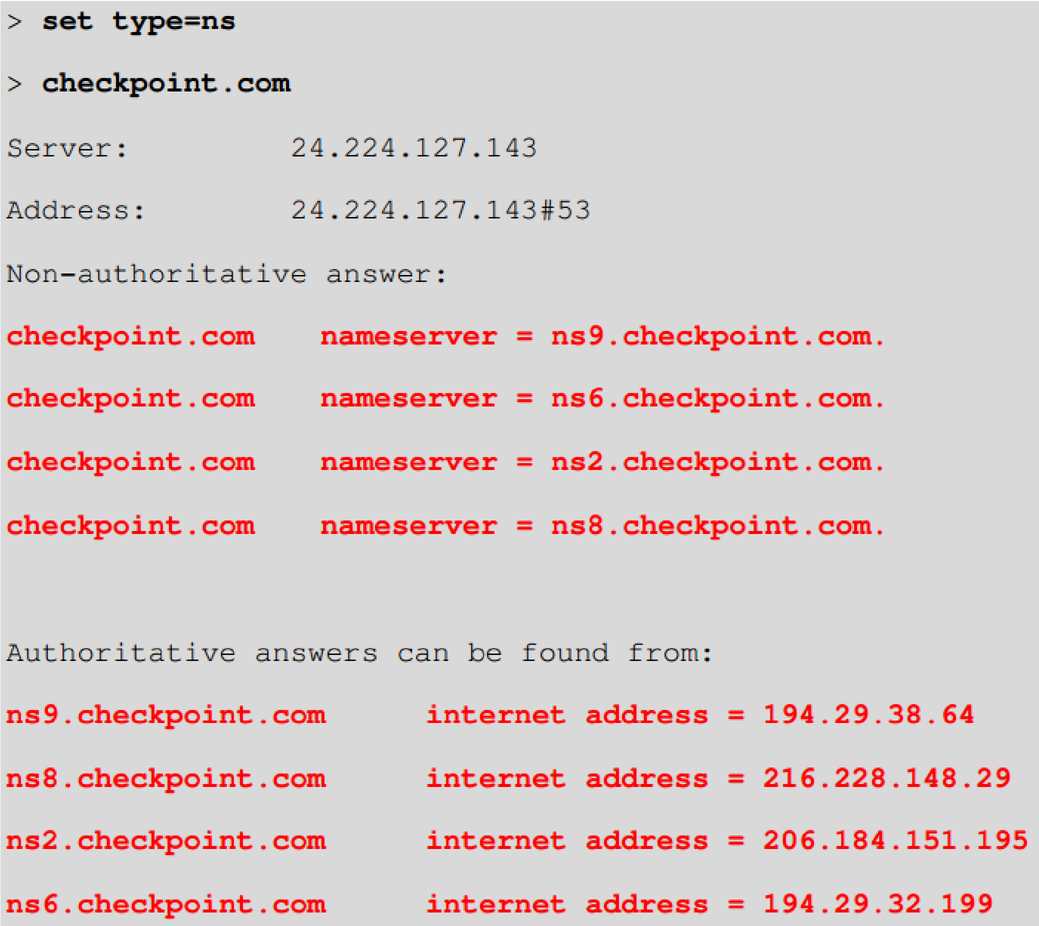
- Can also specify mail server



```
> set type=mx
> checkpoint.com
Server:         24.224.127.143
Address:        24.224.127.143#53
Non-authoritative answer:
checkpoint.com      mail exchanger = 12 sami.checkpoint.com.
checkpoint.com      mail exchanger = 15 usmail-as.zonelabs.com.

Authoritative answers can be found from:
sami.checkpoint.com internet address = 194.29.38.66
usmail-as.zonelabs.com    internet address = 208.185.174.190
```

nslookup options

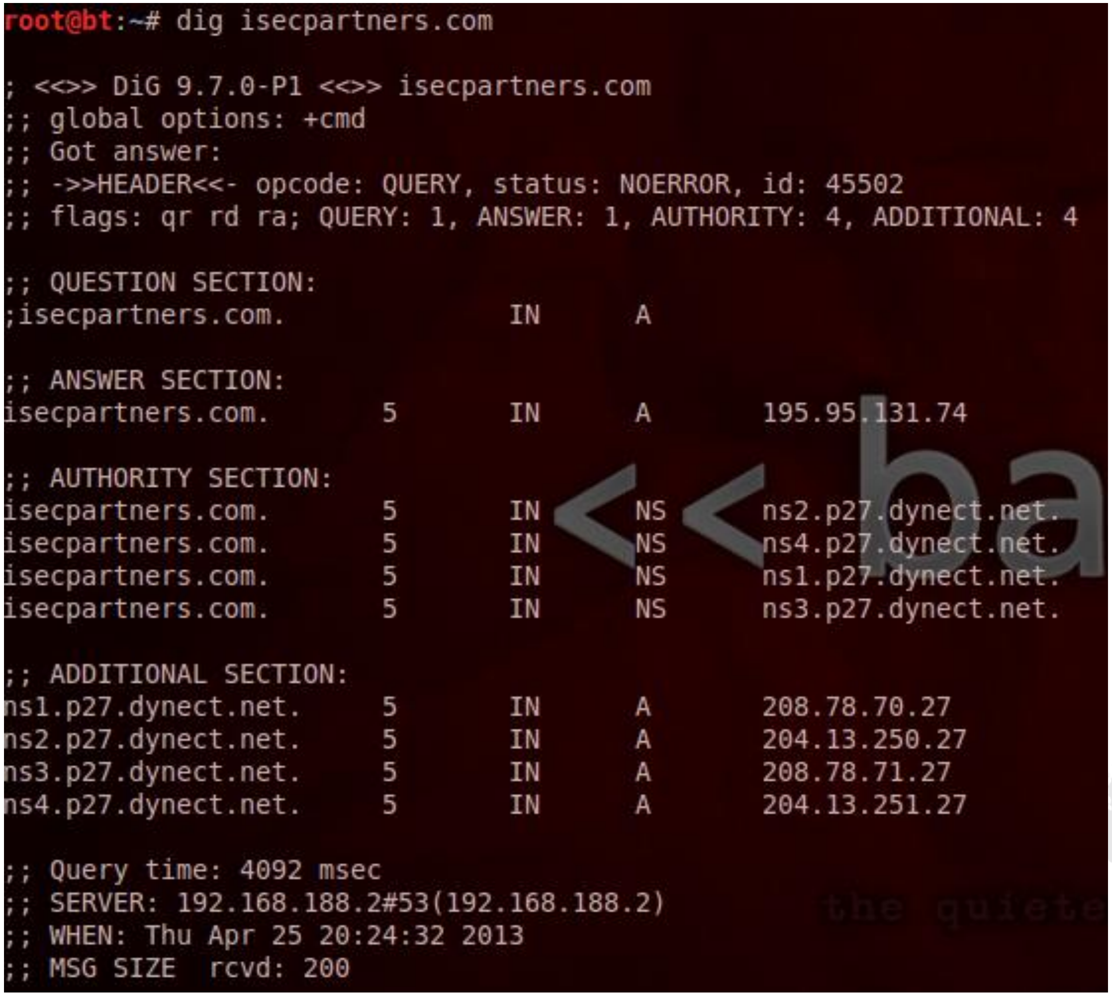
- Nameservers!



```
> set type=ns
> checkpoint.com
Server:         24.224.127.143
Address:        24.224.127.143#53
Non-authoritative answer:
checkpoint.com    nameserver = ns9.checkpoint.com.
checkpoint.com    nameserver = ns6.checkpoint.com.
checkpoint.com    nameserver = ns2.checkpoint.com.
checkpoint.com    nameserver = ns8.checkpoint.com.

Authoritative answers can be found from:
ns9.checkpoint.com     internet address = 194.29.38.64
ns8.checkpoint.com     internet address = 216.228.148.29
ns2.checkpoint.com     internet address = 206.184.151.195
ns6.checkpoint.com     internet address = 194.29.32.199
```

dig

- Powerful DNS client



```
root@bt:~# dig isecpartners.com

; <<>> DiG 9.7.0-P1 <<>> isecpartners.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45502
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;isecpartners.com.              IN      A

;; ANSWER SECTION:
isecpartners.com.       5       IN      A       195.95.131.74

;; AUTHORITY SECTION:
isecpartners.com.       5       IN      NS      ns2.p27.dynect.net.
isecpartners.com.       5       IN      NS      ns4.p27.dynect.net.
isecpartners.com.       5       IN      NS      ns1.p27.dynect.net.
isecpartners.com.       5       IN      NS      ns3.p27.dynect.net.

;; ADDITIONAL SECTION:
ns1.p27.dynect.net.     5       IN      A       208.78.70.27
ns2.p27.dynect.net.     5       IN      A       204.13.250.27
ns3.p27.dynect.net.     5       IN      A       208.78.71.27
ns4.p27.dynect.net.     5       IN      A       204.13.251.27

;; Query time: 4092 msec
;; SERVER: 192.168.188.2#53(192.168.188.2)
;; WHEN: Thu Apr 25 20:24:32 2013
;; MSG SIZE  rcvd: 200
```

dnsenum

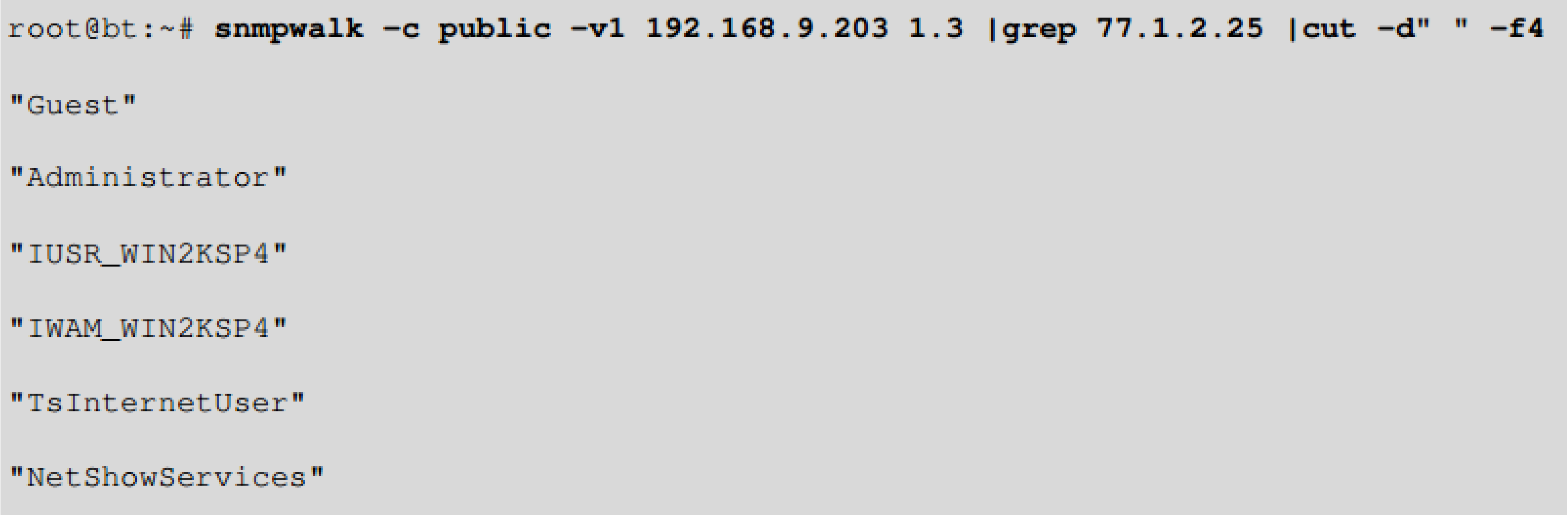
- Automate a lot of the previous actions together in one command
- Brute forces name lookups
- Zone transfers
- Also scrapes Google for info

SNMP

- Management protocol for monitoring and configuring servers and network devices
- Has a “private” string that it uses for Authentication and Authorization
- Most of the time the string is “Public” or is in plaintext on the network
- Even if the string is different, the company has to be using SNMPv3 for any real cryptographic security.
- Contains TONS of information about devices

snmpwalk

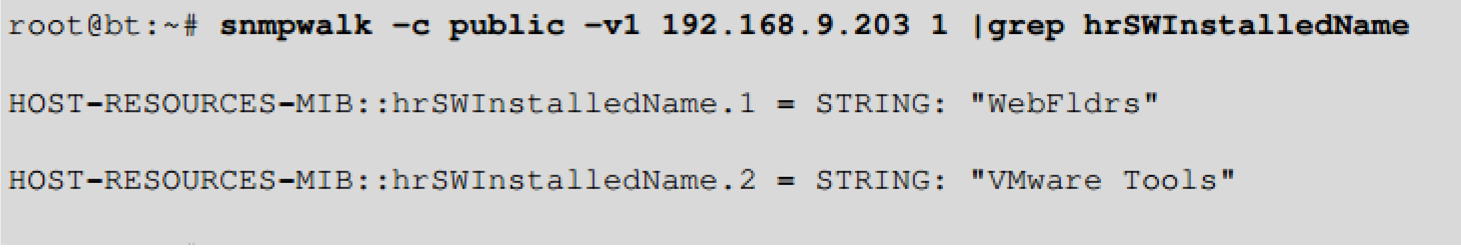
- Enumerate users



```
root@bt:~# snmpwalk -c public -v1 192.168.9.203 1.3 |grep 77.1.2.25 |cut -d" " -f4

"Guest"

"Administrator"

"IUSR_WIN2KSP4"

"IWAM_WIN2KSP4"

"TsInternetUser"

"NetShowServices"
```

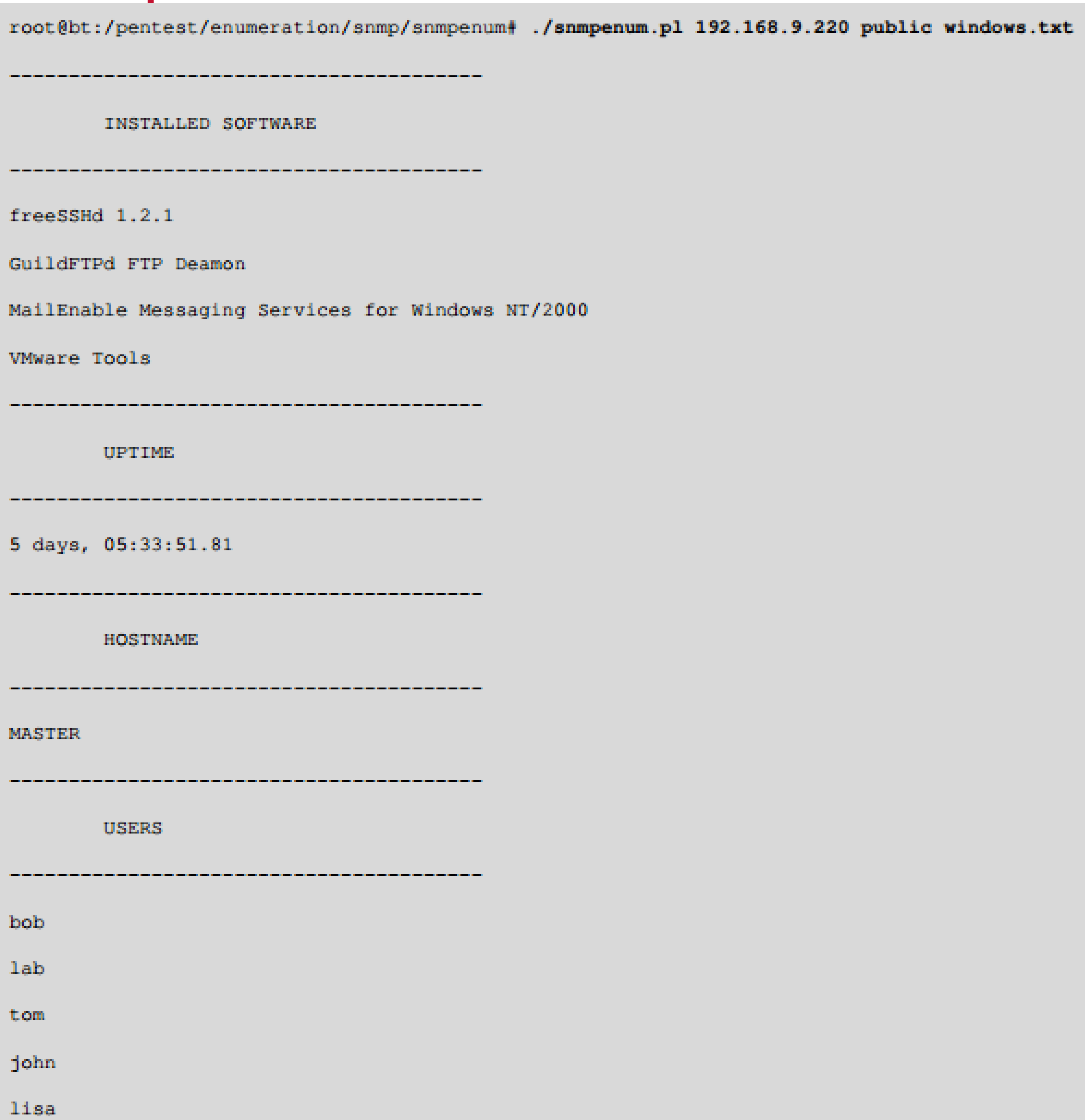
snmpwalk

- Enumerate Software



```
root@bt:~# snmpwalk -c public -v1 192.168.9.203 1 |grep hrSWInstalledName

HOST-RESOURCES-MIB::hrSWInstalledName.1 = STRING: "WebFldrs"

HOST-RESOURCES-MIB::hrSWInstalledName.2 = STRING: "VMware Tools"
```

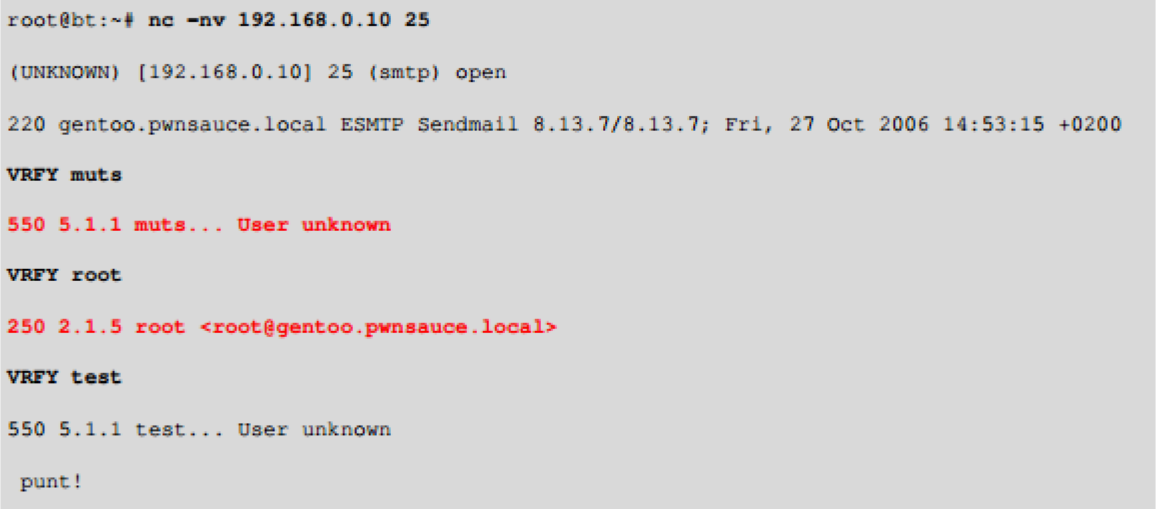
snmpenum



```
root@bt:/pentest/enumeration/snmp/snmpenum# ./snmpenum.pl 192.168.9.220 public windows.txt

----------------------------------------

        INSTALLED SOFTWARE

----------------------------------------

freeSSHd 1.2.1

GuildFTPd FTP Deamon

MailEnable Messaging Services for Windows NT/2000

VMware Tools

----------------------------------------

        UPTIME

----------------------------------------

5 days, 05:33:51.81

----------------------------------------

        HOSTNAME

----------------------------------------

MASTER

----------------------------------------

        USERS

----------------------------------------

bob

lab

tom

john

lisa
```

SMTP

- Mail servers!
- Can connect to them with Netcat (more info later)



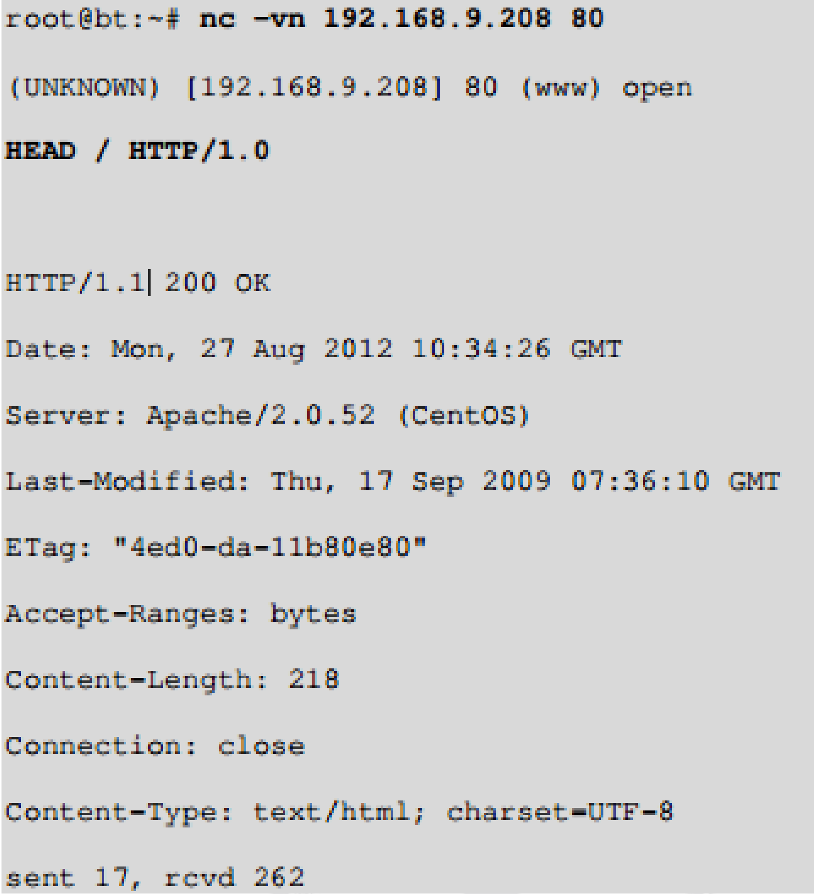
```
root@bt:~# nc -nv 192.168.0.10 25

(UNKNOWN) [192.168.0.10] 25 (smtp) open

220 gentoo.pwnsauce.local ESMTP Sendmail 8.13.7/8.13.7; Fri, 27 Oct 2006 14:53:15 +0200

VRFY muts

550 5.1.1 muts... User unknown

VRFY root

250 2.1.5 root <root@gentoo.pwnsauce.local>

VRFY test

550 5.1.1 test... User unknown

 punt!
```

netcat

- I am required by security law to say that this is the "hacker's swiss army knife"
- Basically it allows you to connect and send traffic over ports, it can read and write to TCP and UDP ports
- Uses:
  - Check if a port is open or closed (port scanning)
  - Read banners (version checking)
  - Connect to a service manually

Netcat examples

- Port Scanning
- Banner grabbing
- Service connecting



```
root@bt:~# nc -vn 192.168.9.208 80
(UNKNOWN) [192.168.9.208] 80 (www) open
HEAD / HTTP/1.0

HTTP/1.1| 200 OK
Date: Mon, 27 Aug 2012 10:34:26 GMT
Server: Apache/2.0.52 (CentOS)
Last-Modified: Thu, 17 Sep 2009 07:36:10 GMT
ETag: "4ed0-da-11b80e80"
Accept-Ranges: bytes
Content-Length: 218
Connection: close
Content-Type: text/html; charset=UTF-8
sent 17, rcvd 262
```

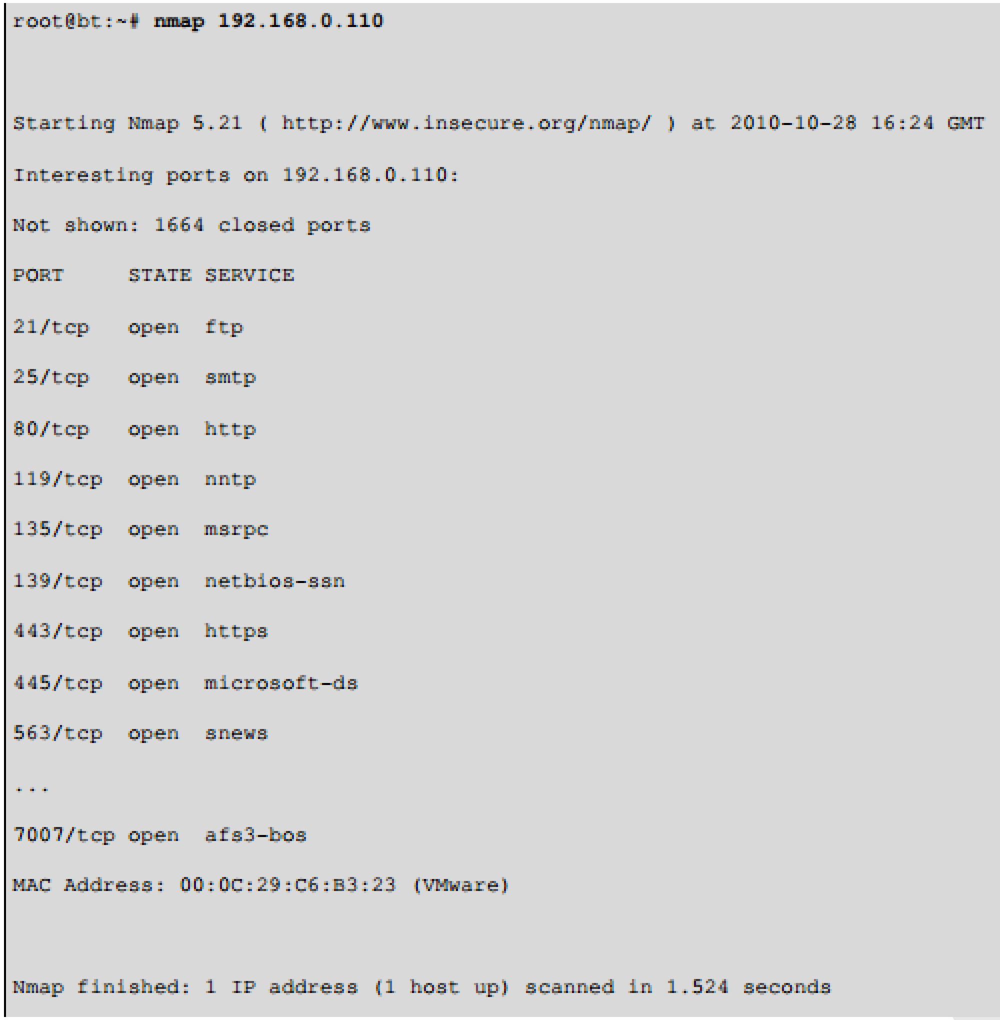
Port Scanning

- Scan port to see what is open, what is closed, and what can be determined by those ports

Nmap

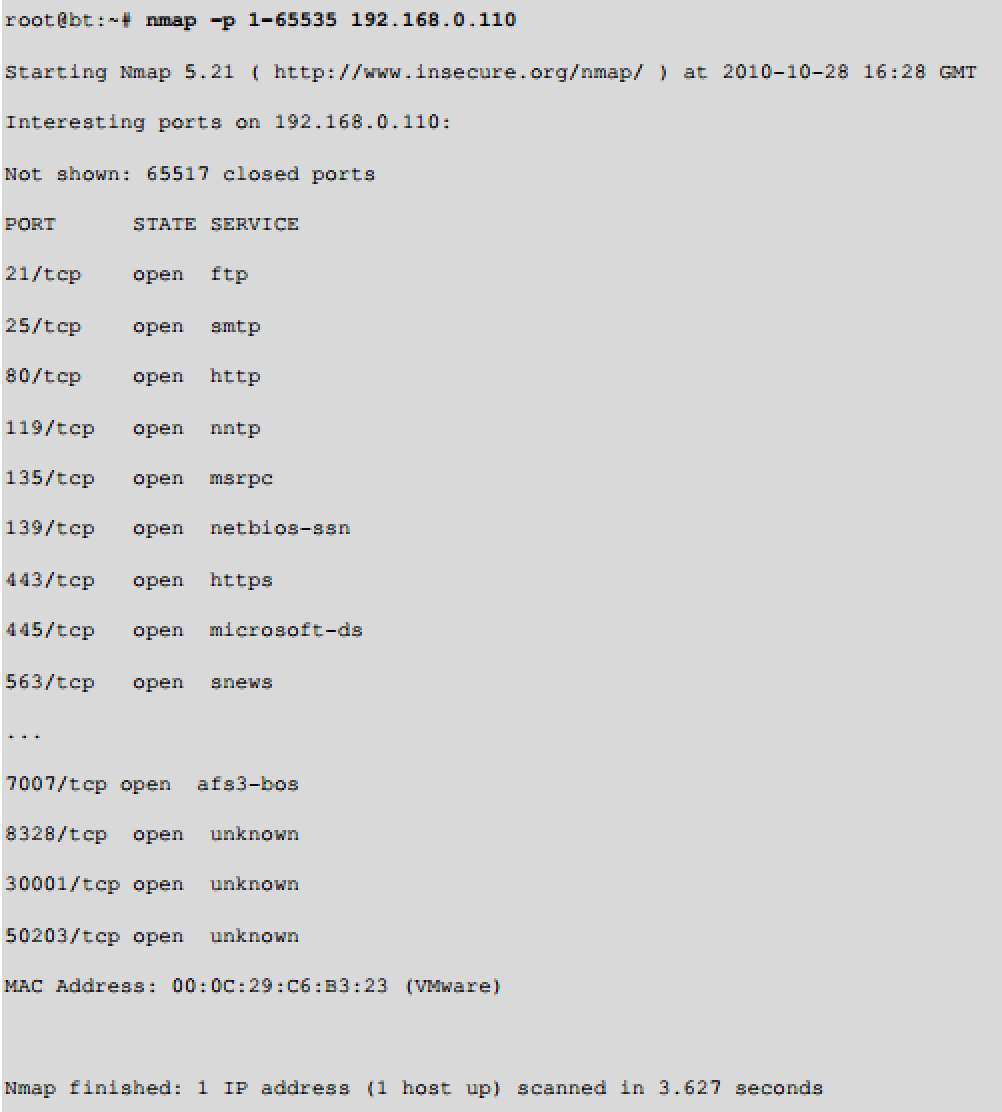
- Most popular port scanner
  - TCP or UDP
  - Also has some vulnerability scanning options now with NSE
  - Version/OS detection

Nmap Examples



```
root@bt:~# nmap 192.168.0.110


Starting Nmap 5.21 ( http://www.insecure.org/nmap/ ) at 2010-10-28 16:24 GMT
Interesting ports on 192.168.0.110:
Not shown: 1664 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
80/tcp   open  http
119/tcp  open  nntp
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
563/tcp  open  snews
...
7007/tcp open  afs3-bos
MAC Address: 00:0C:29:C6:B3:23 (VMware)


Nmap finished: 1 IP address (1 host up) scanned in 1.524 seconds
```

nmap – full TCP scan



```
root@bt:~# nmap -p 1-65535 192.168.0.110

Starting Nmap 5.21 ( http://www.insecure.org/nmap/ ) at 2010-10-28 16:28 GMT

Interesting ports on 192.168.0.110:

Not shown: 65517 closed ports

PORT      STATE  SERVICE

21/tcp    open   ftp

25/tcp    open   smtp

80/tcp    open   http

119/tcp   open   nntp

135/tcp   open   msrpc

139/tcp   open   netbios-ssn

443/tcp   open   https

445/tcp   open   microsoft-ds

563/tcp   open   snews

...

7007/tcp open   afs3-bos

8328/tcp  open   unknown

30001/tcp open   unknown

50203/tcp open   unknown

MAC Address: 00:0C:29:C6:B3:23 (VMware)


Nmap finished: 1 IP address (1 host up) scanned in 3.627 seconds
```

Other nmap examples

- Scripting Engine
  - nmap 192.168.9.221 --script smb-enum-users.nse
- Banner Grabbing
  - nmap -sV 192.168.182.129
- OS Fingerprinting
  - nmap -O 192.168.0.1
- Network sweeping
  - nmap -p 139 192.168.0.*

Attack Vectors

- Vulnerability scanning
- Exploits – exploit-db, metasploit
- Data theft
- DDoS
- Blackmail

Thank You

- Jake Meredith
  - Security Consultant at iSEC Partners
  - jmeredith@isecpartners.com

UK Offices

Manchester - Head Office
Cheltenham
Edinburgh
Leatherhead
London
Thame

European Offices

Amsterdam - Netherlands
Munich – Germany
Zurich - Switzerland

North American Offices

San Francisco
Atlanta
New York
Seattle

Australian Offices

Sydney