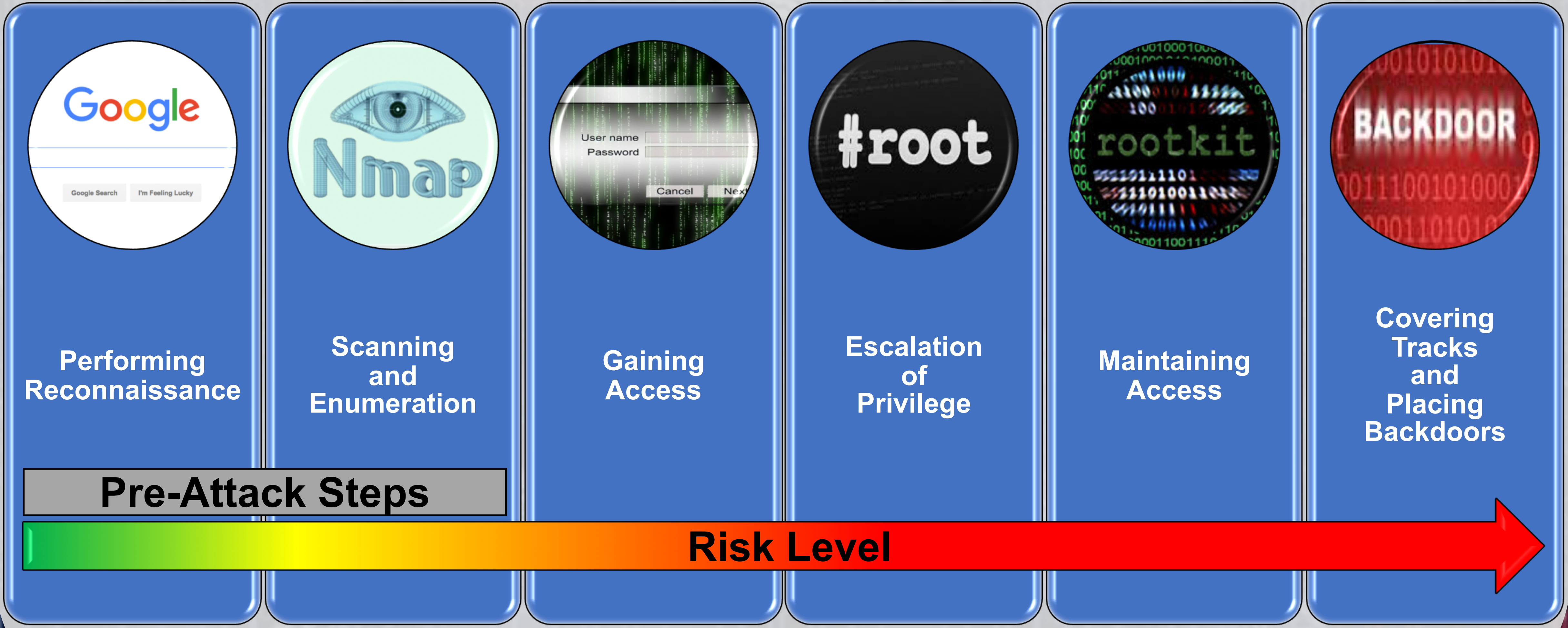
Reconnaissance Phase

(…I can see you but you can’t see me)

Attacker’s Methodology



Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

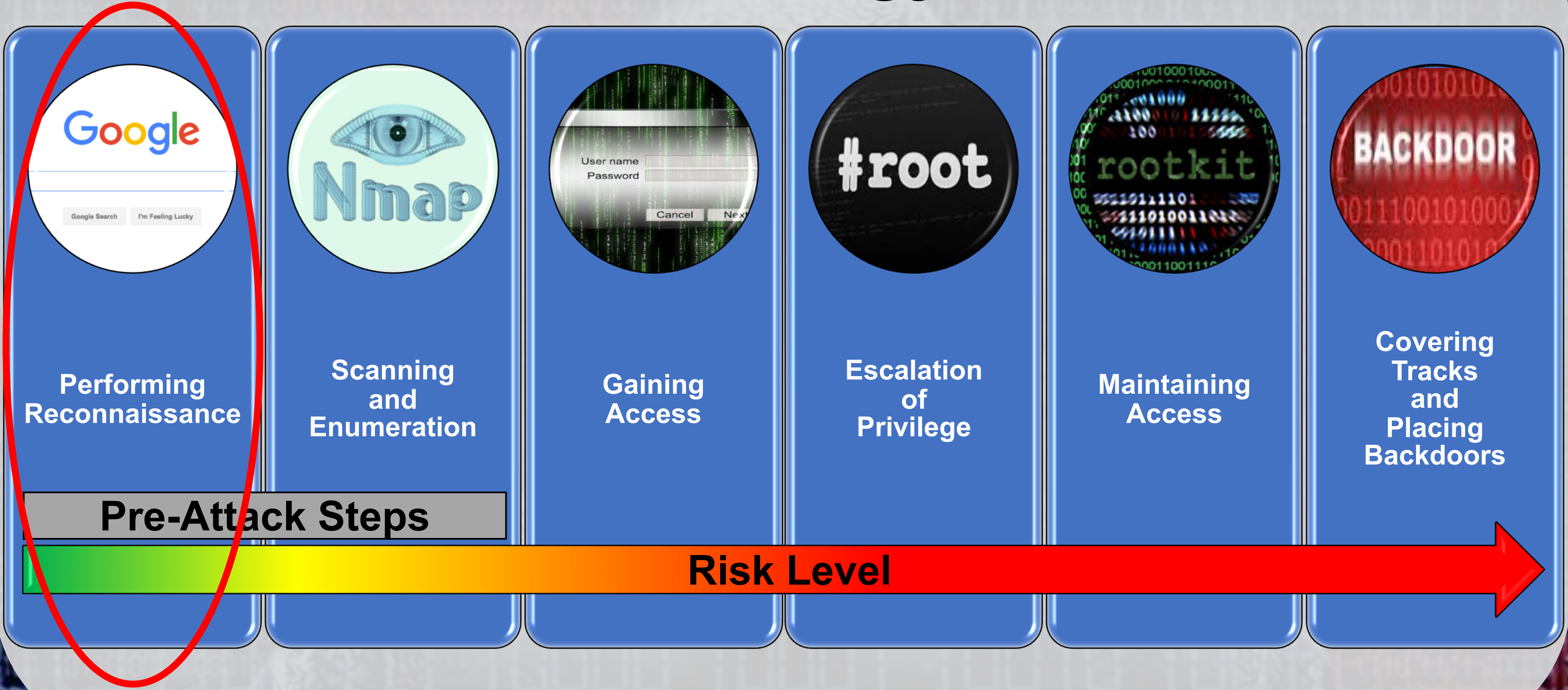
Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

Attacker’s Methodology



Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

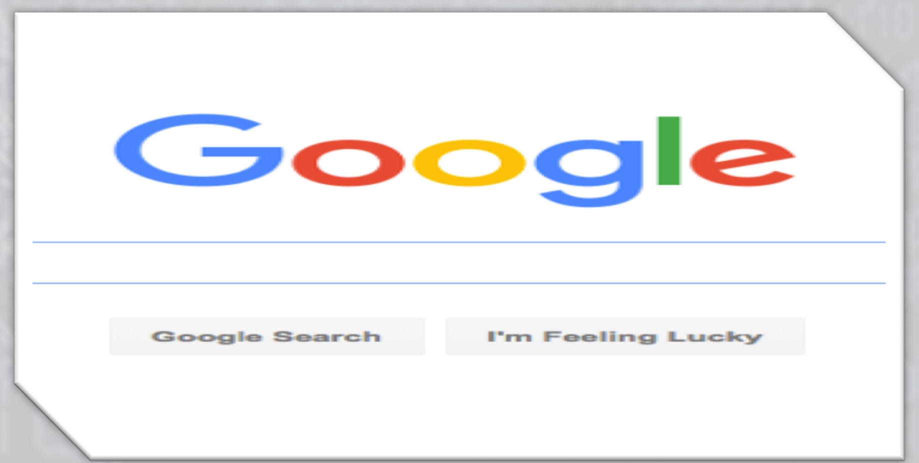
Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

Phase 1 - Performing Reconnaissance



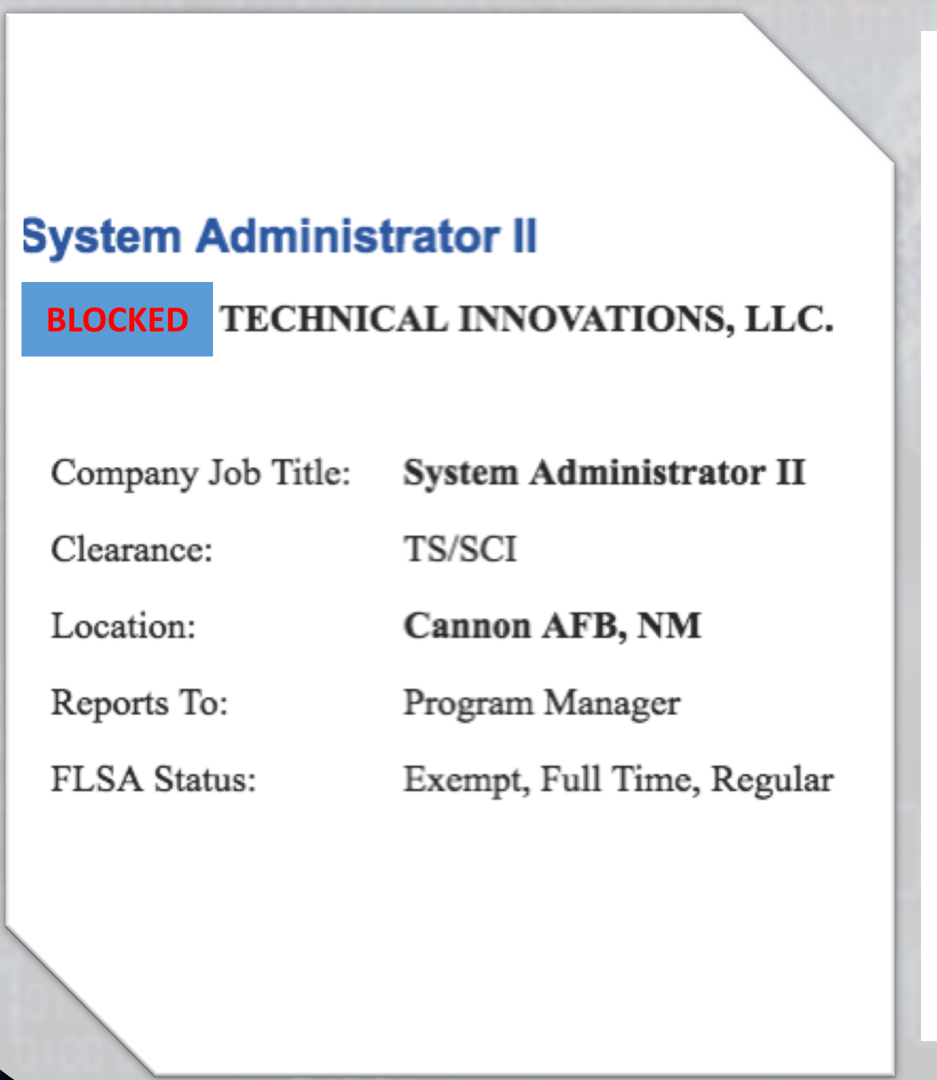
- Systematic attempt to locate, gather, identify, and record information about target
- Also called “Footprinting”
- Reconnaissance techniques include:
  - Internet or open-source research
  - Social engineering
  - Dumpster diving
  - Email harvesting
- Only <u>PASSIVE</u> information gathering occurs

Types of Information Desired

What types of information would be helpful to gather?

- Phone numbers
- Contact names
- Email addresses
- Security-related information
- Information Systems used
- Job postings
- Resumes

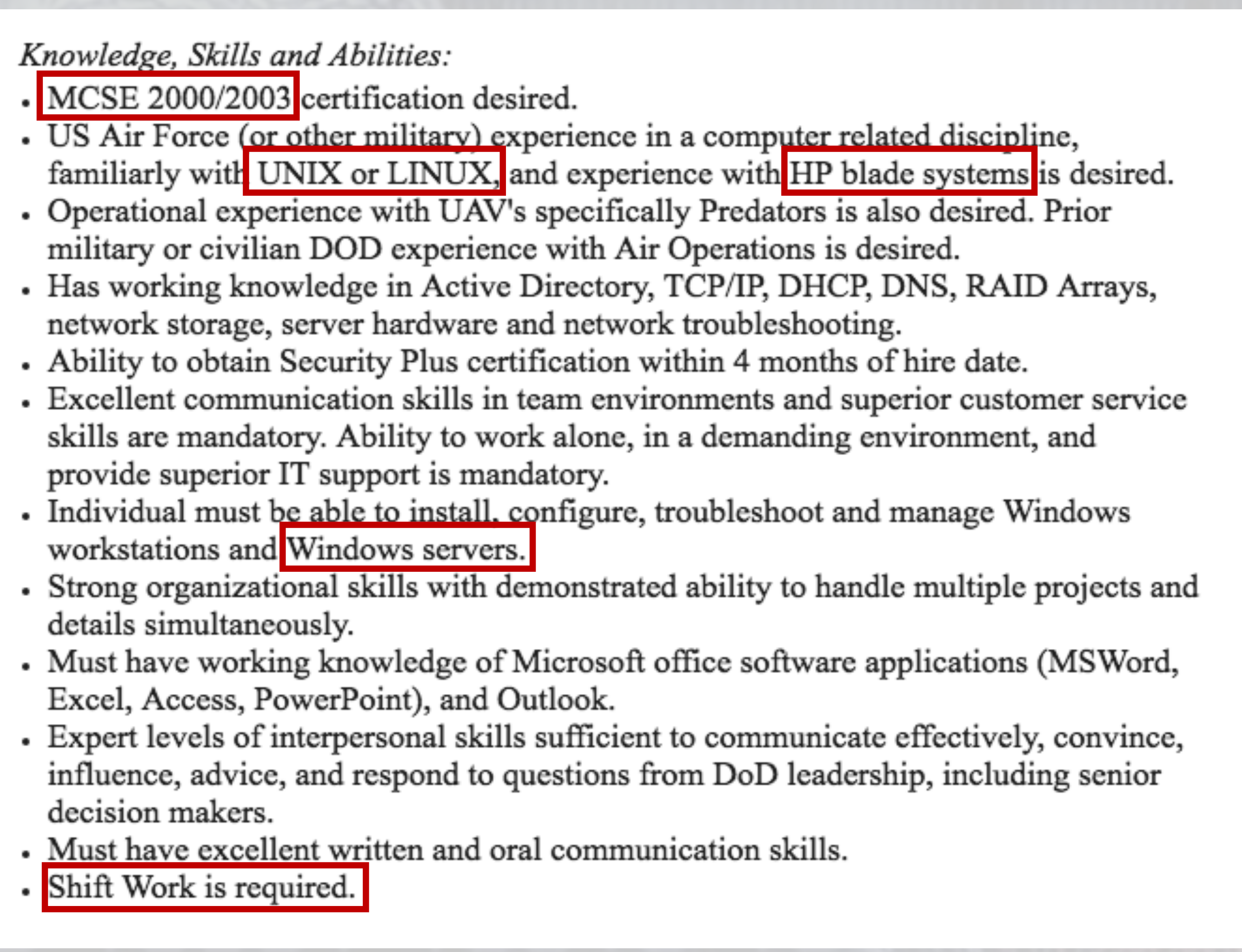
Job Postings



System Administrator II

BLOCKED TECHNICAL INNOVATIONS, LLC.

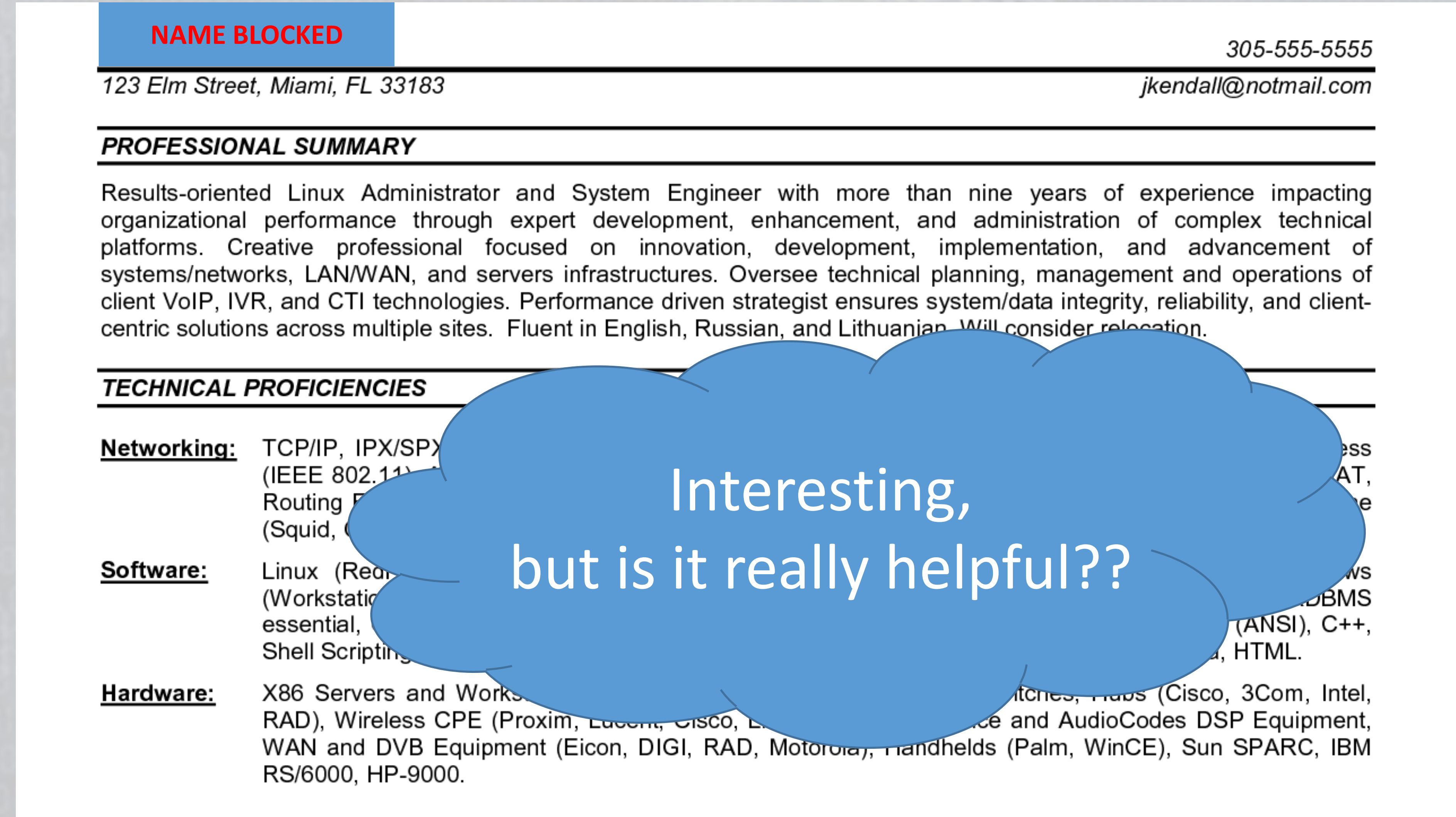
Company Job Title:	**System Administrator II**
Clearance:	TS/SCI
Location:	**Cannon AFB, NM**
Reports To:	Program Manager
FLSA Status:	Exempt, Full Time, Regular



Knowledge, Skills and Abilities:

- MCSE 2000/2003 certification desired.
- US Air Force (or other military) experience in a computer related discipline, familiarly with UNIX or LINUX, and experience with HP blade systems is desired.
- Operational experience with UAV's specifically Predators is also desired. Prior military or civilian DOD experience with Air Operations is desired.
- Has working knowledge in Active Directory, TCP/IP, DHCP, DNS, RAID Arrays, network storage, server hardware and network troubleshooting.
- Ability to obtain Security Plus certification within 4 months of hire date.
- Excellent communication skills in team environments and superior customer service skills are mandatory. Ability to work alone, in a demanding environment, and provide superior IT support is mandatory.
- Individual must be able to install, configure, troubleshoot and manage Windows workstations and Windows servers.
- Strong organizational skills with demonstrated ability to handle multiple projects and details simultaneously.
- Must have working knowledge of Microsoft office software applications (MSWord, Excel, Access, PowerPoint), and Outlook.
- Expert levels of interpersonal skills sufficient to communicate effectively, convince, influence, advice, and respond to questions from DoD leadership, including senior decision makers.
- Must have excellent written and oral communication skills.
- Shift Work is required.

Resumes



NAME BLOCKED

305-555-5555

123 Elm Street, Miami, FL 33183

jkendall@notmail.com

PROFESSIONAL SUMMARY

Results-oriented Linux Administrator and System Engineer with more than nine years of experience impacting organizational performance through expert development, enhancement, and administration of complex technical platforms. Creative professional focused on innovation, development, implementation, and advancement of systems/networks, LAN/WAN, and servers infrastructures. Oversee technical planning, management and operations of client VoIP, IVR, and CTI technologies. Performance driven strategist ensures system/data integrity, reliability, and client-centric solutions across multiple sites. Fluent in English, Russian, and Lithuanian. Will consider relocation.

TECHNICAL PROFICIENCIES

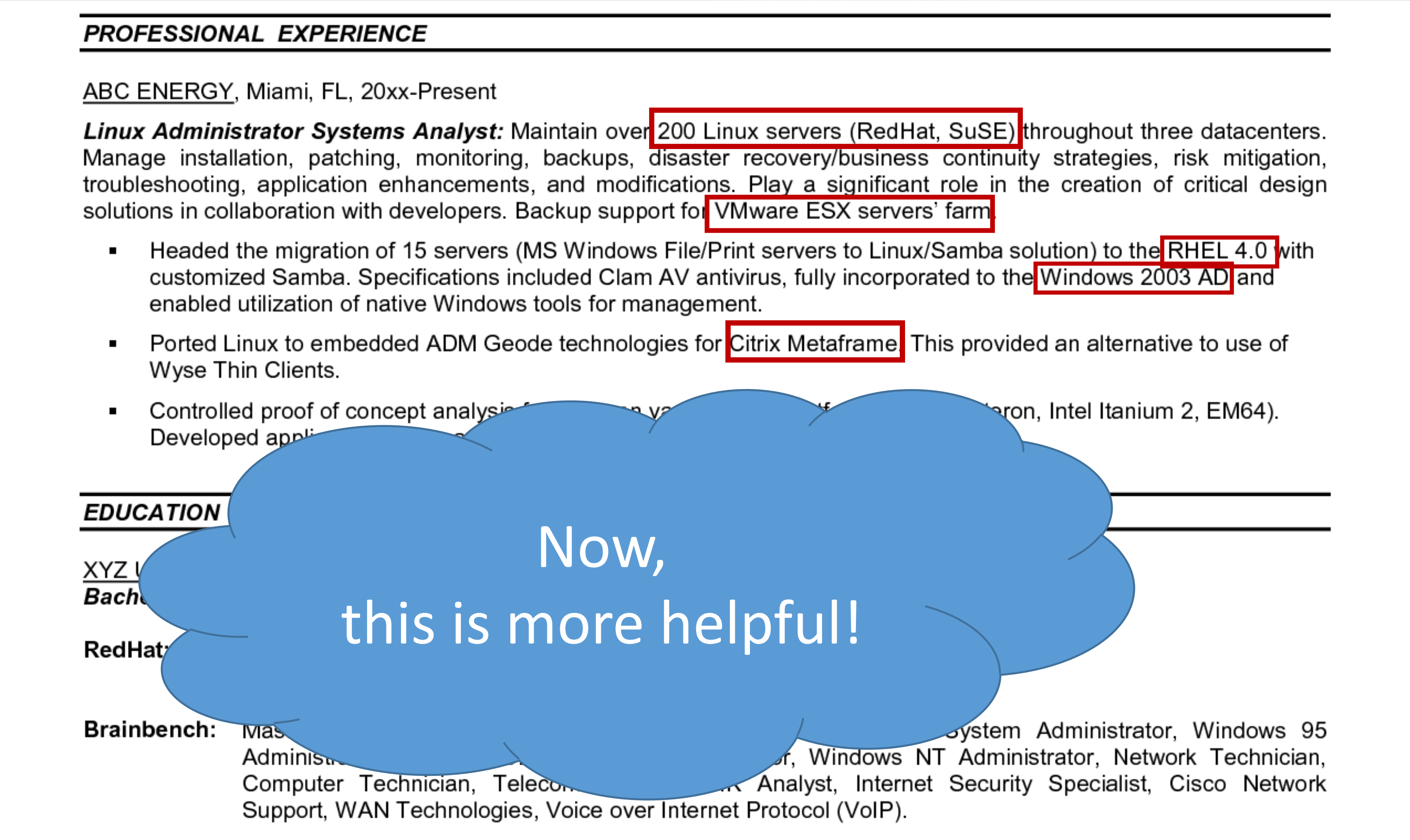
Networking: TCP/IP, IPX/SPX … ess (IEEE 802.11) … AT, Routing … e (Squid, …

Software: Linux (Red … ws (Workstatio … DBMS essential, … (ANSI), C++, Shell Scripti… , HTML.

Hardware: X86 Servers and Works… itches, Hubs (Cisco, 3Com, Intel, RAD), Wireless CPE (Proxim, Lucent, Cisco, L… ce and AudioCodes DSP Equipment, WAN and DVB Equipment (Eicon, DIGI, RAD, Motorola), Handhelds (Palm, WinCE), Sun SPARC, IBM RS/6000, HP-9000.

Interesting,
but is it really helpful??

Resumes



PROFESSIONAL EXPERIENCE

ABC ENERGY, Miami, FL, 20xx-Present

Linux Administrator Systems Analyst: Maintain over 200 Linux servers (RedHat, SuSE) throughout three datacenters. Manage installation, patching, monitoring, backups, disaster recovery/business continuity strategies, risk mitigation, troubleshooting, application enhancements, and modifications. Play a significant role in the creation of critical design solutions in collaboration with developers. Backup support for VMware ESX servers' farm.

- Headed the migration of 15 servers (MS Windows File/Print servers to Linux/Samba solution) to the RHEL 4.0 with customized Samba. Specifications included Clam AV antivirus, fully incorporated to the Windows 2003 AD and enabled utilization of native Windows tools for management.
- Ported Linux to embedded ADM Geode technologies for Citrix Metaframe. This provided an alternative to use of Wyse Thin Clients.
- Controlled proof of concept analysis f n va tf teron, Intel Itanium 2, EM64). Developed appl

EDUCATION

XYZ U

Bach

RedHat:

Brainbench: Mas System Administrator, Windows 95 Administ r, Windows NT Administrator, Network Technician, Computer Technician, Telecon k Analyst, Internet Security Specialist, Cisco Network Support, WAN Technologies, Voice over Internet Protocol (VoIP).

Now,
this is more helpful!

Tools Used for Reconnaissance

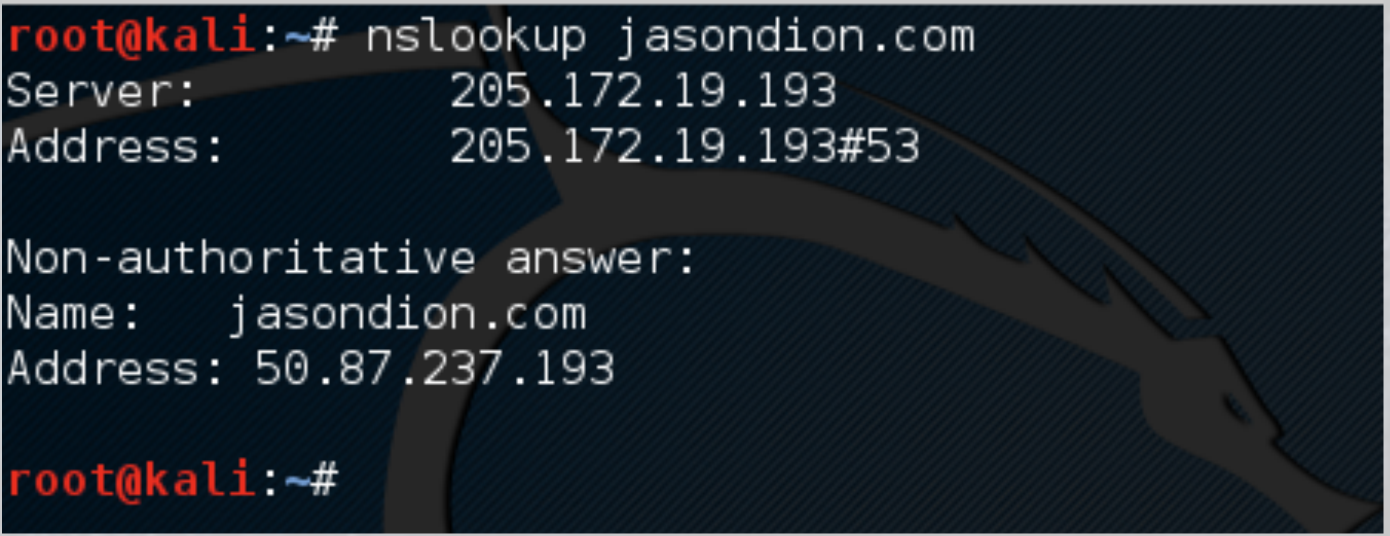
Many tools exist:

- Nslookup
- Traceroute
- Ping
- Whois
- Domain Dossier
- Email Dossier
- Google
- Social Networking
- Discover
- Maltego

nslookup

- **nslookup** (name server lookup) resolves a fully qualified domain name (FQDN) to an IP address

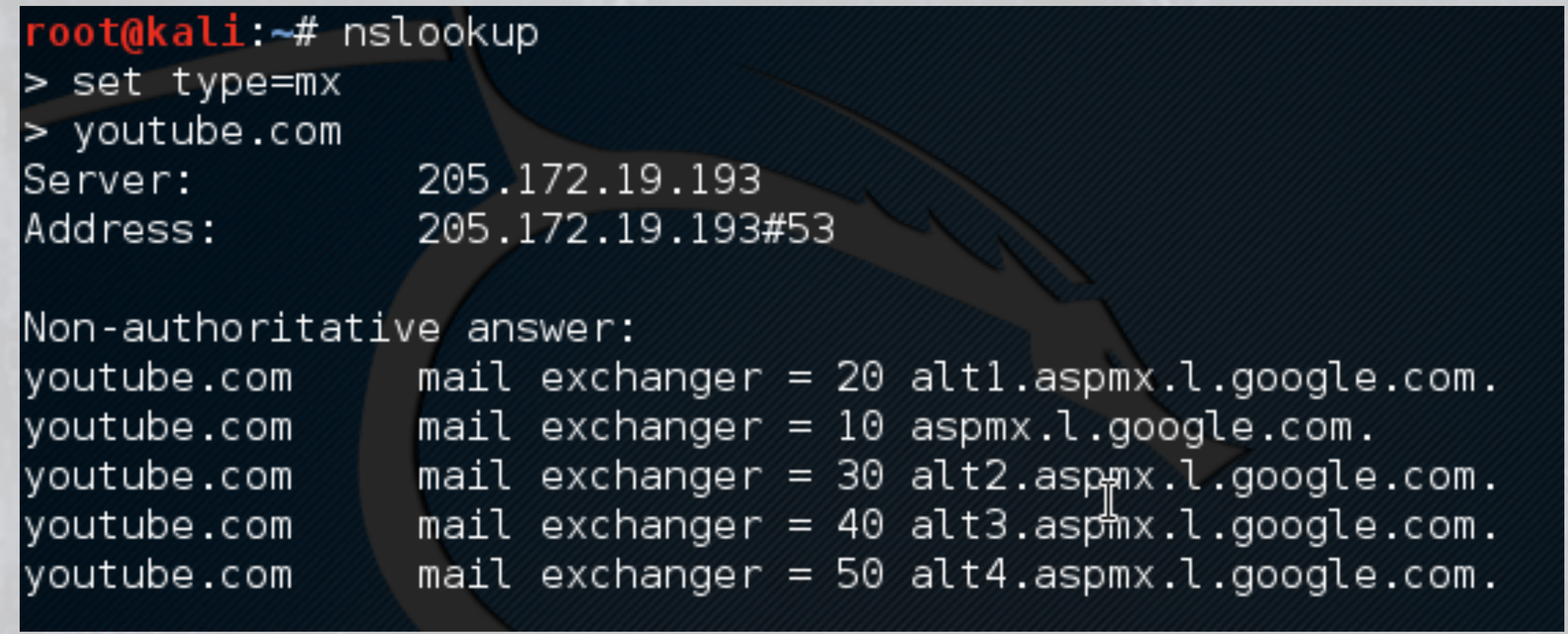
- **nslookup www.jasondion.com**
  - Non-interactive mode, provides IP address for a given domain name (provides more details than in Windows)



```
root@kali:~# nslookup jasondion.com
Server:         205.172.19.193
Address:        205.172.19.193#53

Non-authoritative answer:
Name:   jasondion.com
Address: 50.87.237.193

root@kali:~#
```

nslookup

- **nslookup <enter>**
  - Loads interactive mode, allows for detailed control of the environment, including which name server to use for name resolution/lookup



```
root@kali:~# nslookup
> set type=mx
> youtube.com
Server:         205.172.19.193
Address:        205.172.19.193#53

Non-authoritative answer:
youtube.com     mail exchanger = 20 alt1.aspmx.l.google.com.
youtube.com     mail exchanger = 10 aspmx.l.google.com.
youtube.com     mail exchanger = 30 alt2.aspmx.l.google.com.
youtube.com     mail exchanger = 40 alt3.aspmx.l.google.com.
youtube.com     mail exchanger = 50 alt4.aspmx.l.google.com.
```

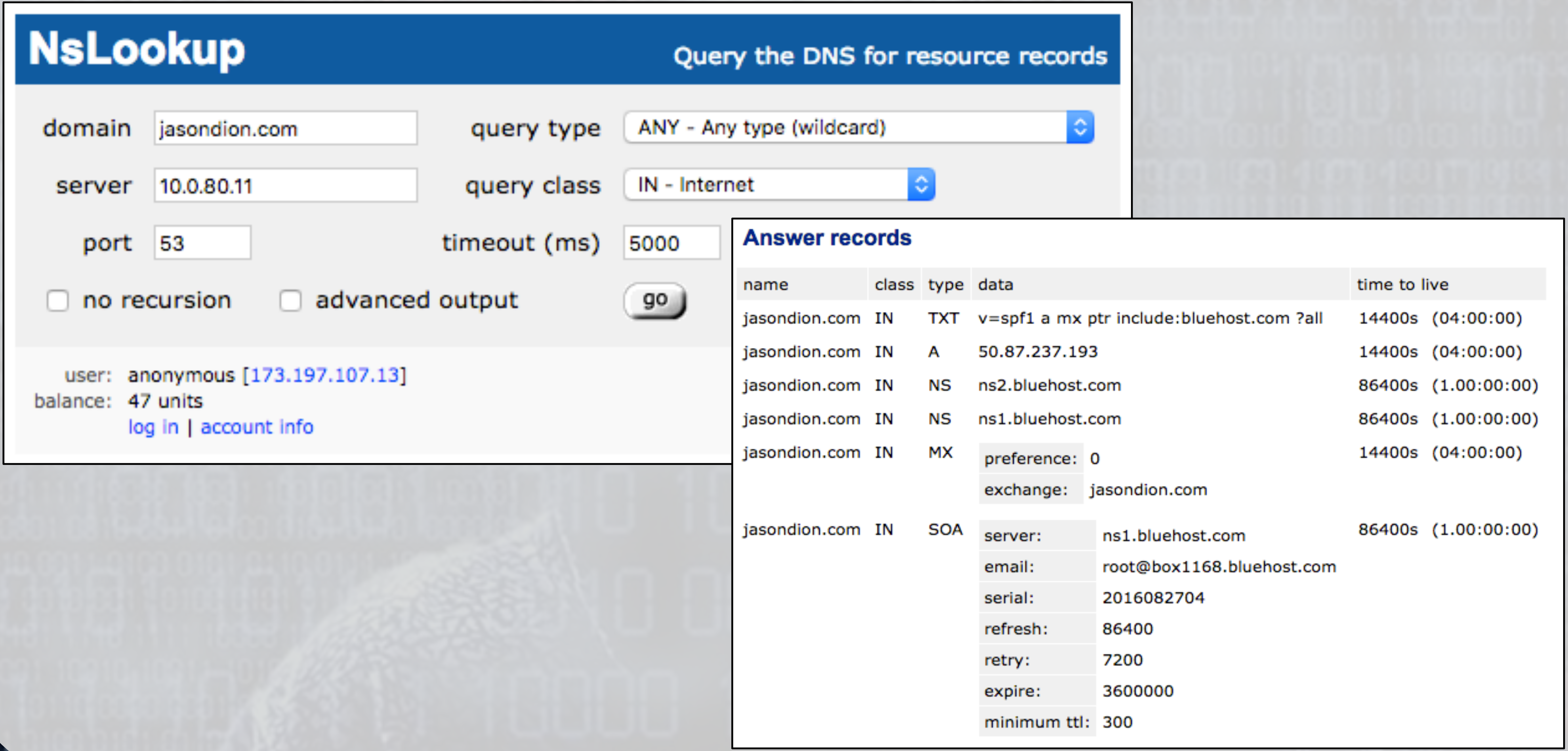
nslookup

Option	Description
A or AAAA	Provides a computer's IP address
CNAME	Provides a canonical name for an alias
HINFO	Provides a server's CPU and type of operating system
MB	Provides a mailbox domain name
MINFO	Provides mailbox or mail list information
MX	Provides the mail exchanger
NS	Provides a DNS name server for the named zone
PTR	Provides a computer name if the query is an IP address
SOA	Provides the start-of-authority for a DNS zone
TXT	Provides the text information
UID	Specifies the user identifier

Use http://network-tools.com or http://centralops.net to perform your nslookup anonymously

(Remain passive during the Reconnaissance Phase)

nslookup



NsLookup

Query the DNS for resource records

domain	jasondion.com	query type	ANY - Any type (wildcard)
server	10.0.80.11	query class	IN - Internet
port	53	timeout (ms)	5000

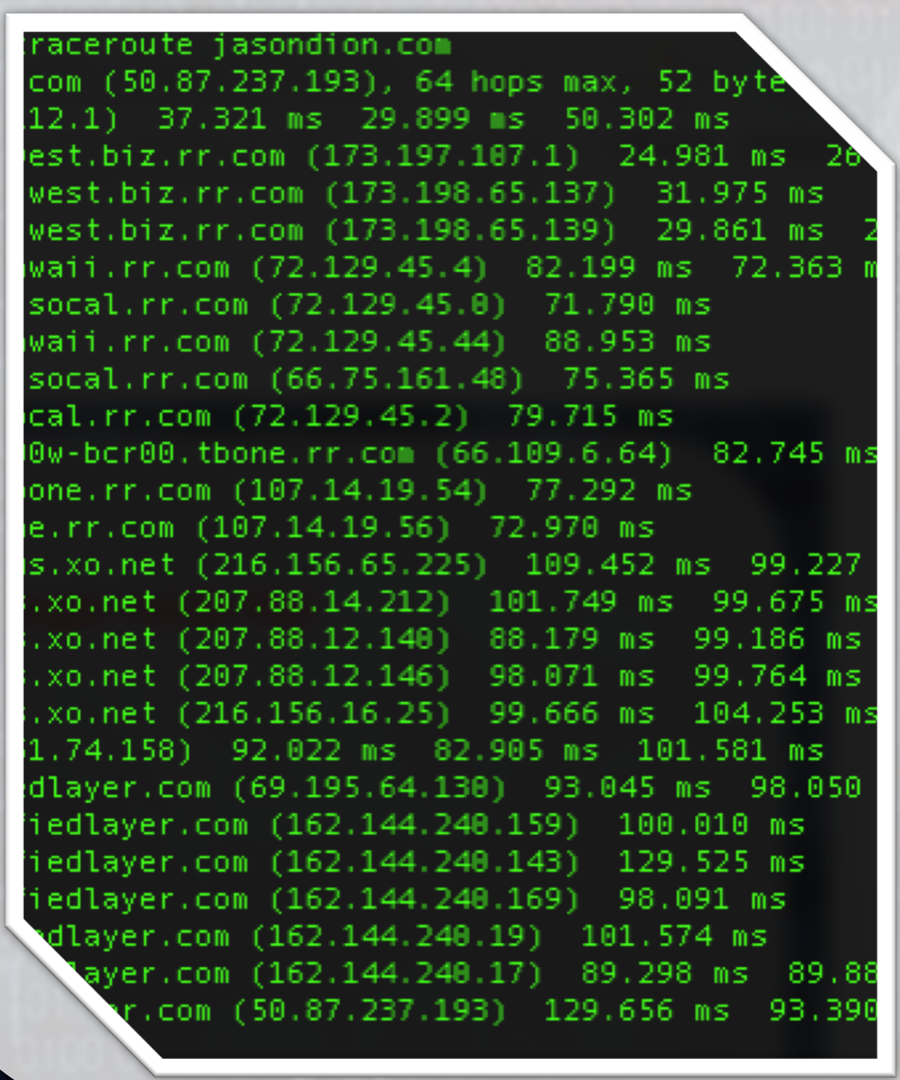
□ no recursion □ advanced output go

user: anonymous [173.197.107.13]
balance: 47 units
log in | account info

Answer records

name	class	type	data		time to live
jasondion.com	IN	TXT	v=spf1 a mx ptr include:bluehost.com ?all		14400s (04:00:00)
jasondion.com	IN	A	50.87.237.193		14400s (04:00:00)
jasondion.com	IN	NS	ns2.bluehost.com		86400s (1.00:00:00)
jasondion.com	IN	NS	ns1.bluehost.com		86400s (1.00:00:00)
jasondion.com	IN	MX	preference:	0	14400s (04:00:00)
			exchange:	jasondion.com	
jasondion.com	IN	SOA	server:	ns1.bluehost.com	86400s (1.00:00:00)
			email:	root@box1168.bluehost.com	
			serial:	2016082704	
			refresh:	86400	
			retry:	7200	
			expire:	3600000	
			minimum ttl:	300	

traceroute



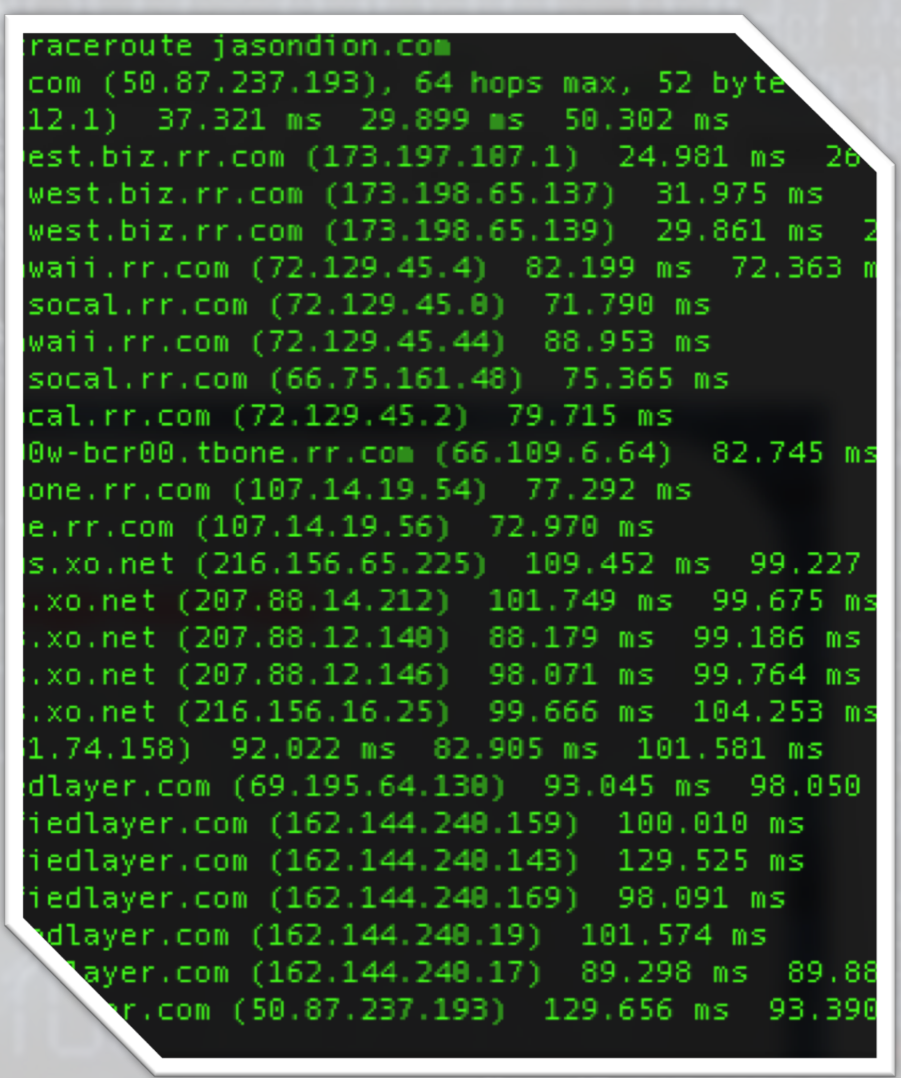
```
raceroute jasondion.com
com (50.87.237.193), 64 hops max, 52 byte
12.1)  37.321 ms  29.899 ms  50.302 ms
est.biz.rr.com (173.197.107.1)  24.981 ms  26
west.biz.rr.com (173.198.65.137)  31.975 ms
west.biz.rr.com (173.198.65.139)  29.861 ms  2
waii.rr.com (72.129.45.4)  82.199 ms  72.363 m
socal.rr.com (72.129.45.0)  71.790 ms
waii.rr.com (72.129.45.44)  88.953 ms
socal.rr.com (66.75.161.48)  75.365 ms
cal.rr.com (72.129.45.2)  79.715 ms
0w-bcr00.tbone.rr.com (66.109.6.64)  82.745 ms
one.rr.com (107.14.19.54)  77.292 ms
e.rr.com (107.14.19.56)  72.970 ms
s.xo.net (216.156.65.225)  109.452 ms  99.227
.xo.net (207.88.14.212)  101.749 ms  99.675 ms
.xo.net (207.88.12.140)  88.179 ms  99.186 ms
.xo.net (207.88.12.146)  98.071 ms  99.764 ms
.xo.net (216.156.16.25)  99.666 ms  104.253 ms
1.74.158)  92.022 ms  82.905 ms  101.581 ms
dlayer.com (69.195.64.130)  93.045 ms  98.050
iedlayer.com (162.144.240.159)  100.010 ms
iedlayer.com (162.144.240.143)  129.525 ms
iedlayer.com (162.144.240.169)  98.091 ms
dlayer.com (162.144.240.19)  101.574 ms
ayer.com (162.144.240.17)  89.298 ms  89.88
r.com (50.87.237.193)  129.656 ms  93.390
```

traceroute displays the path between your device (the source) and the destination IP address, showing each route hop along the path

- **traceroute 209.85.135.99**
  - Displays the routers between your computer and the computer at 209.85.135.99
- **traceroute www.google.com**
  - Displays the routers between your computer and www.google.com

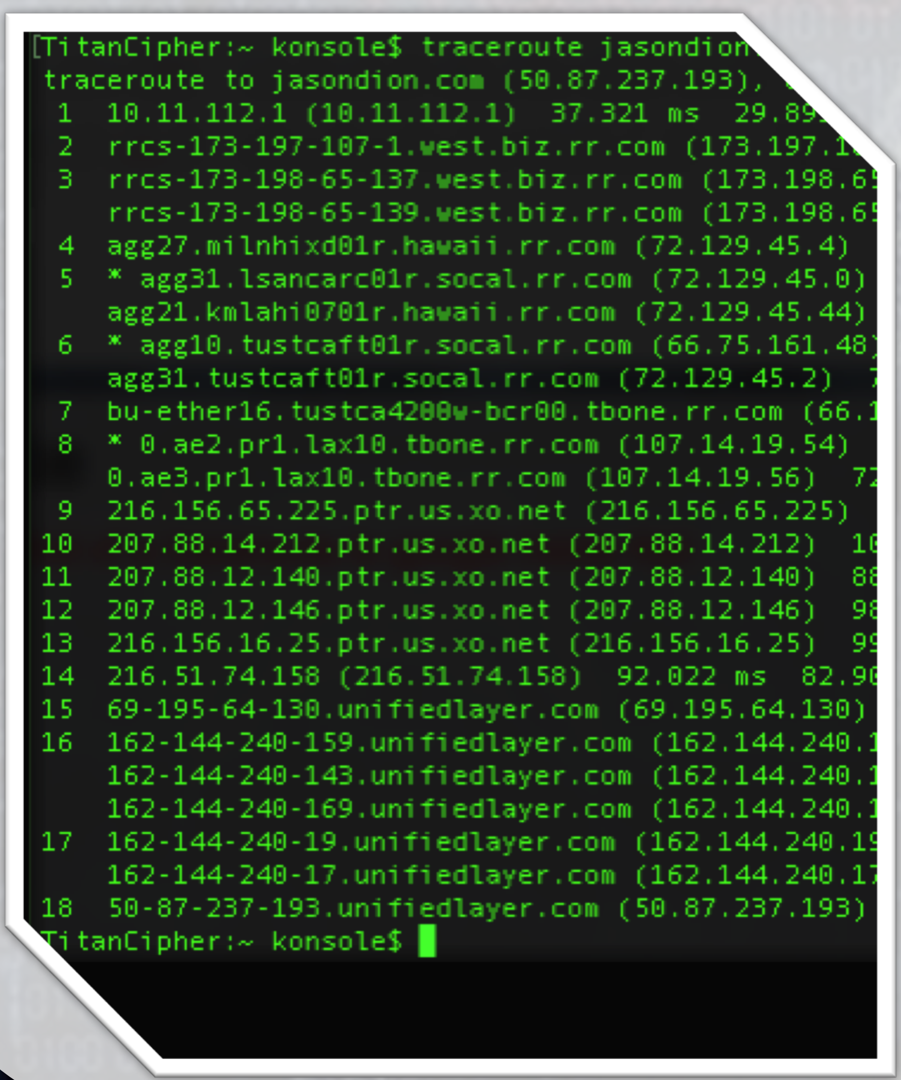
traceroute

- Increases the "time-to-live" (TTL) value of each following set of packets sent to target
  - First three packets sent have TTL value of 1
  - Next three packets sent have TTL value of 2
- When a packet passes through a host, normally the host decrements the TTL value by one, and forwards the packet to the next host in the route
- When a packet with a TTL of 1 reaches a host, the host discards the packet and sends an ICMP time exceeded (type 11) packet back to the sender



```
raceroute jasondion.com
com (50.87.237.193), 64 hops max, 52 byte
12.1)  37.321 ms  29.899 ms  50.302 ms
est.biz.rr.com (173.197.107.1)  24.981 ms  26
west.biz.rr.com (173.198.65.137)  31.975 ms
west.biz.rr.com (173.198.65.139)  29.861 ms  2
waii.rr.com (72.129.45.4)  82.199 ms  72.363 m
socal.rr.com (72.129.45.0)  71.790 ms
waii.rr.com (72.129.45.44)  88.953 ms
socal.rr.com (66.75.161.48)  75.365 ms
cal.rr.com (72.129.45.2)  79.715 ms
0w-bcr00.tbone.rr.com (66.109.6.64)  82.745 ms
one.rr.com (107.14.19.54)  77.292 ms
e.rr.com (107.14.19.56)  72.970 ms
s.xo.net (216.156.65.225)  109.452 ms  99.227
.xo.net (207.88.14.212)  101.749 ms  99.675 ms
.xo.net (207.88.12.140)  88.179 ms  99.186 ms
.xo.net (207.88.12.146)  98.071 ms  99.764 ms
.xo.net (216.156.16.25)  99.666 ms  104.253 ms
1.74.158)  92.022 ms  82.905 ms  101.581 ms
dlayer.com (69.195.64.130)  93.045 ms  98.050
iedlayer.com (162.144.240.159)  100.010 ms
iedlayer.com (162.144.240.143)  129.525 ms
iedlayer.com (162.144.240.169)  98.091 ms
dlayer.com (162.144.240.19)  101.574 ms
ayer.com (162.144.240.17)  89.298 ms  89.88
r.com (50.87.237.193)  129.656 ms  93.390
```

traceroute



```
[TitanCipher:~ konsole$ traceroute jasondion
 traceroute to jasondion.com (50.87.237.193),
 1  10.11.112.1 (10.11.112.1)  37.321 ms  29.89
 2  rrcs-173-197-107-1.west.biz.rr.com (173.197.1
 3  rrcs-173-198-65-137.west.biz.rr.com (173.198.6
    rrcs-173-198-65-139.west.biz.rr.com (173.198.6
 4  agg27.milnhixd01r.hawaii.rr.com (72.129.45.4)
 5  * agg31.lsancarc01r.socal.rr.com (72.129.45.0)
    agg21.kmlahi0701r.hawaii.rr.com (72.129.45.44)
 6  * agg10.tustcaft01r.socal.rr.com (66.75.161.48)
    agg31.tustcaft01r.socal.rr.com (72.129.45.2)  7
 7  bu-ether16.tustca4200w-bcr00.tbone.rr.com (66.1
 8  * 0.ae2.pr1.lax10.tbone.rr.com (107.14.19.54)
    0.ae3.pr1.lax10.tbone.rr.com (107.14.19.56)  72
 9  216.156.65.225.ptr.us.xo.net (216.156.65.225)
10  207.88.14.212.ptr.us.xo.net (207.88.14.212)  10
11  207.88.12.140.ptr.us.xo.net (207.88.12.140)  88
12  207.88.12.146.ptr.us.xo.net (207.88.12.146)  98
13  216.156.16.25.ptr.us.xo.net (216.156.16.25)  99
14  216.51.74.158 (216.51.74.158)  92.022 ms  82.90
15  69-195-64-130.unifiedlayer.com (69.195.64.130)
16  162-144-240-159.unifiedlayer.com (162.144.240.1
    162-144-240-143.unifiedlayer.com (162.144.240.1
    162-144-240-169.unifiedlayer.com (162.144.240.1
17  162-144-240-19.unifiedlayer.com (162.144.240.19
    162-144-240-17.unifiedlayer.com (162.144.240.17
18  50-87-237-193.unifiedlayer.com (50.87.237.193)
TitanCipher:~ konsole$ 
```

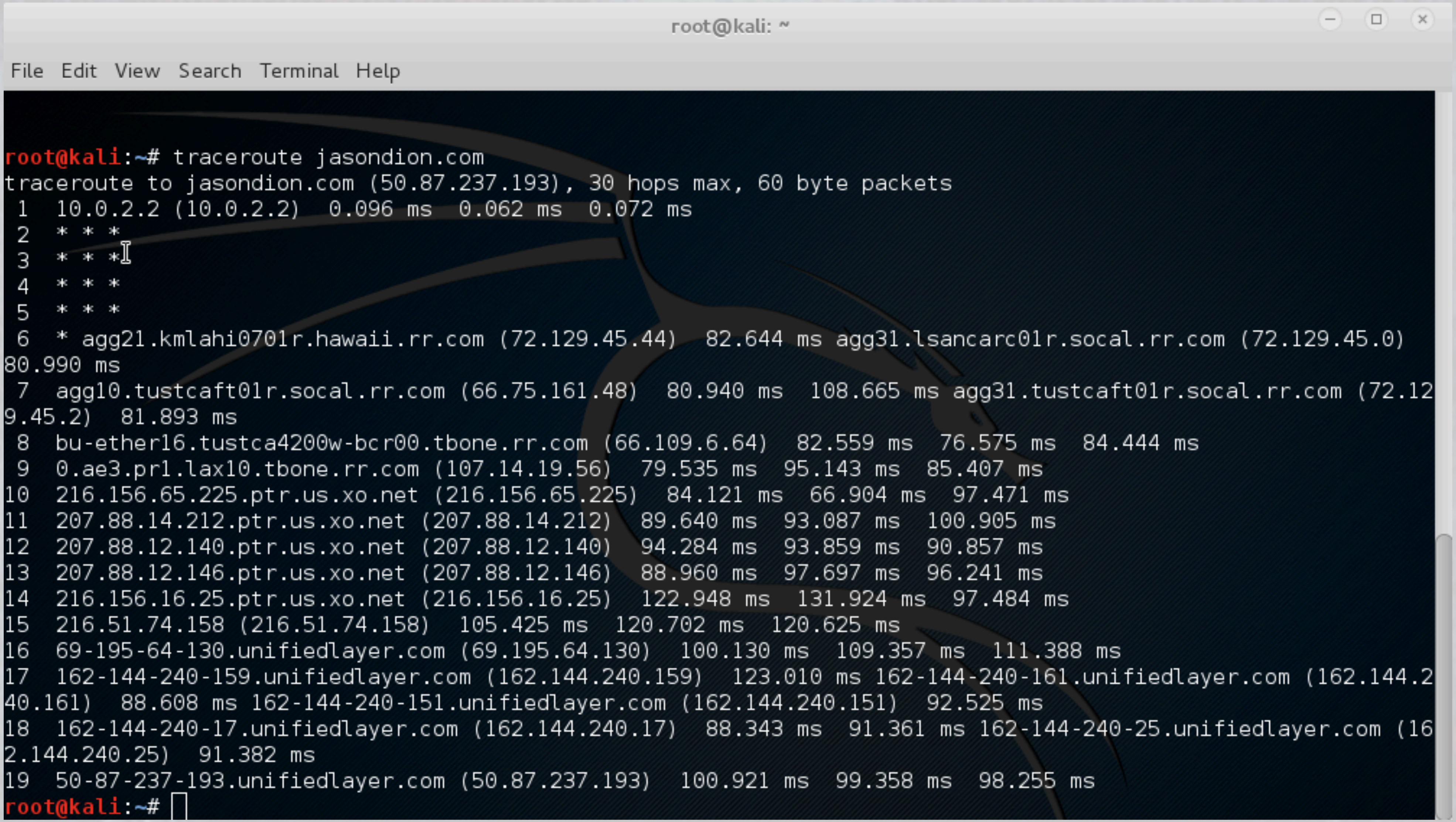
- Three timestamp values returned for each host along the path are the delay (latency) values measured in milliseconds (ms) for each set of packets

- What does latency tell you about your target?

Device	Average Latency
Dial-up Modem	100-150 ms
ISDN Line	40-50 ms
Cellular Modem	50-150 ms
Satellite Modem	650-750 ms
Fiber Optic	5-40 ms
Cable Modem	15-100 ms

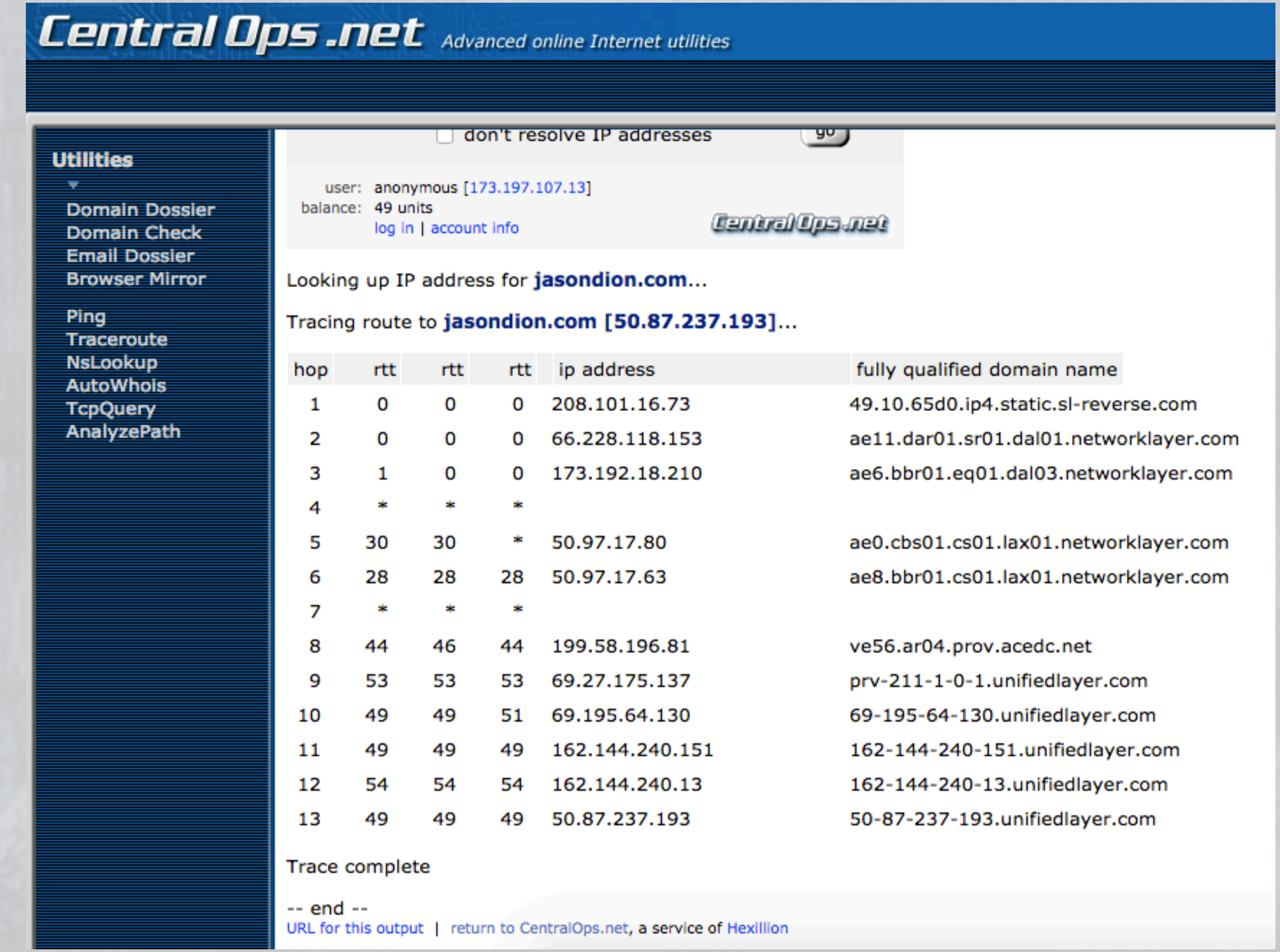
- * * * on a line usually means you found an internal network that is protected by a gateway or firewall

traceroute



```
root@kali:~# traceroute jasondion.com
traceroute to jasondion.com (50.87.237.193), 30 hops max, 60 byte packets
 1  10.0.2.2 (10.0.2.2)  0.096 ms  0.062 ms  0.072 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * agg21.kmlahi0701r.hawaii.rr.com (72.129.45.44)  82.644 ms agg31.lsancarc01r.socal.rr.com (72.129.45.0)
80.990 ms
 7  agg10.tustcaft01r.socal.rr.com (66.75.161.48)  80.940 ms  108.665 ms agg31.tustcaft01r.socal.rr.com (72.12
9.45.2)  81.893 ms
 8  bu-ether16.tustca4200w-bcr00.tbone.rr.com (66.109.6.64)  82.559 ms  76.575 ms  84.444 ms
 9  0.ae3.pr1.lax10.tbone.rr.com (107.14.19.56)  79.535 ms  95.143 ms  85.407 ms
10  216.156.65.225.ptr.us.xo.net (216.156.65.225)  84.121 ms  66.904 ms  97.471 ms
11  207.88.14.212.ptr.us.xo.net (207.88.14.212)  89.640 ms  93.087 ms  100.905 ms
12  207.88.12.140.ptr.us.xo.net (207.88.12.140)  94.284 ms  93.859 ms  90.857 ms
13  207.88.12.146.ptr.us.xo.net (207.88.12.146)  88.960 ms  97.697 ms  96.241 ms
14  216.156.16.25.ptr.us.xo.net (216.156.16.25)  122.948 ms  131.924 ms  97.484 ms
15  216.51.74.158 (216.51.74.158)  105.425 ms  120.702 ms  120.625 ms
16  69-195-64-130.unifiedlayer.com (69.195.64.130)  100.130 ms  109.357 ms  111.388 ms
17  162-144-240-159.unifiedlayer.com (162.144.240.159)  123.010 ms 162-144-240-161.unifiedlayer.com (162.144.2
40.161)  88.608 ms 162-144-240-151.unifiedlayer.com (162.144.240.151)  92.525 ms
18  162-144-240-17.unifiedlayer.com (162.144.240.17)  88.343 ms  91.361 ms 162-144-240-25.unifiedlayer.com (16
2.144.240.25)  91.382 ms
19  50-87-237-193.unifiedlayer.com (50.87.237.193)  100.921 ms  99.358 ms  98.255 ms
root@kali:~# 
```

traceroute



user: anonymous [173.197.107.13]
balance: 49 units
log in | account info

Looking up IP address for **jasondion.com**...

Tracing route to **jasondion.com [50.87.237.193]**...

hop	rtt	rtt	rtt	ip address	fully qualified domain name
1	0	0	0	208.101.16.73	49.10.65d0.ip4.static.sl-reverse.com
2	0	0	0	66.228.118.153	ae11.dar01.sr01.dal01.networklayer.com
3	1	0	0	173.192.18.210	ae6.bbr01.eq01.dal03.networklayer.com
4	*	*	*		
5	30	30	*	50.97.17.80	ae0.cbs01.cs01.lax01.networklayer.com
6	28	28	28	50.97.17.63	ae8.bbr01.cs01.lax01.networklayer.com
7	*	*	*		
8	44	46	44	199.58.196.81	ve56.ar04.prov.acedc.net
9	53	53	53	69.27.175.137	prv-211-1-0-1.unifiedlayer.com
10	49	49	51	69.195.64.130	69-195-64-130.unifiedlayer.com
11	49	49	49	162.144.240.151	162-144-240-151.unifiedlayer.com
12	54	54	54	162.144.240.13	162-144-240-13.unifiedlayer.com
13	49	49	49	50.87.237.193	50-87-237-193.unifiedlayer.com

Trace complete

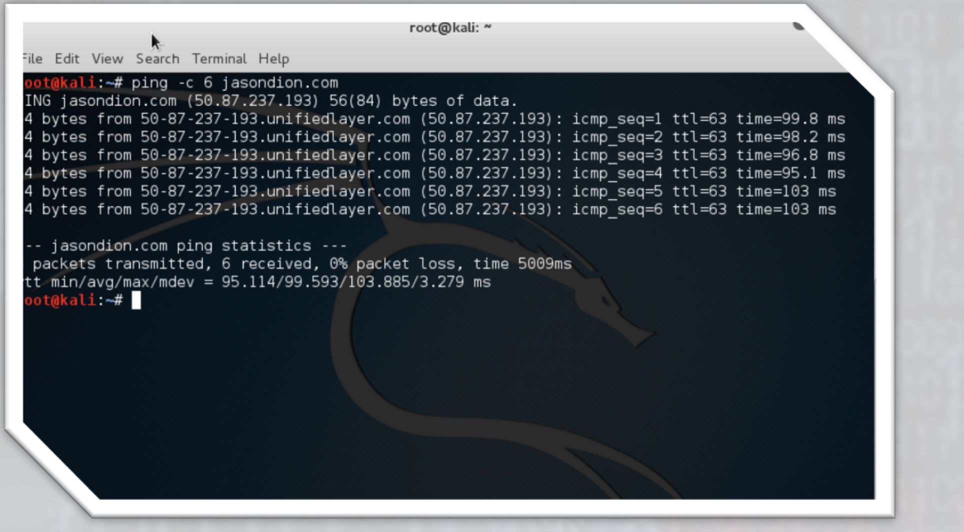
-- end --

URL for this output | return to CentralOps.net, a service of Hexillion

ping

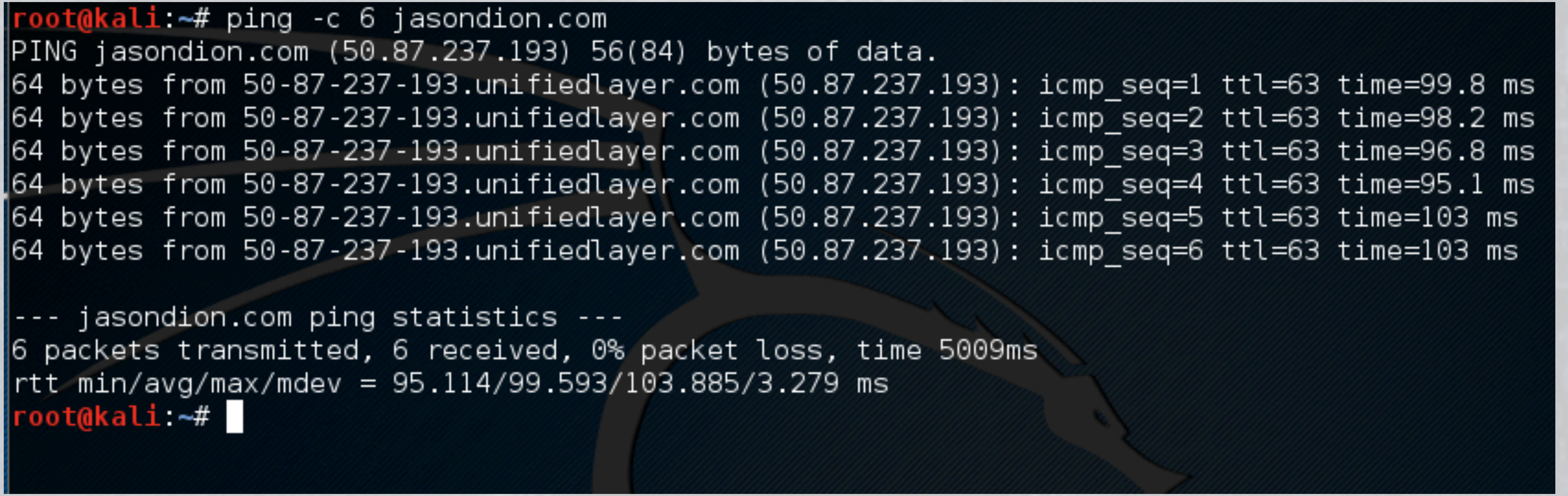
- **ping** is used to check IP connectivity between two network devices and is often used in network troubleshooting

- By default, Linux continuously pings until terminated
  - **ping www.jasondion.com**
    - Ping forever (until user types CTRL+C)
  - **ping –c 10 www.jasondion.com**
    - Ping 10 times, then stop
  - **ping –6 www.jasondion.com**
    - Ping using IPv6 addresses



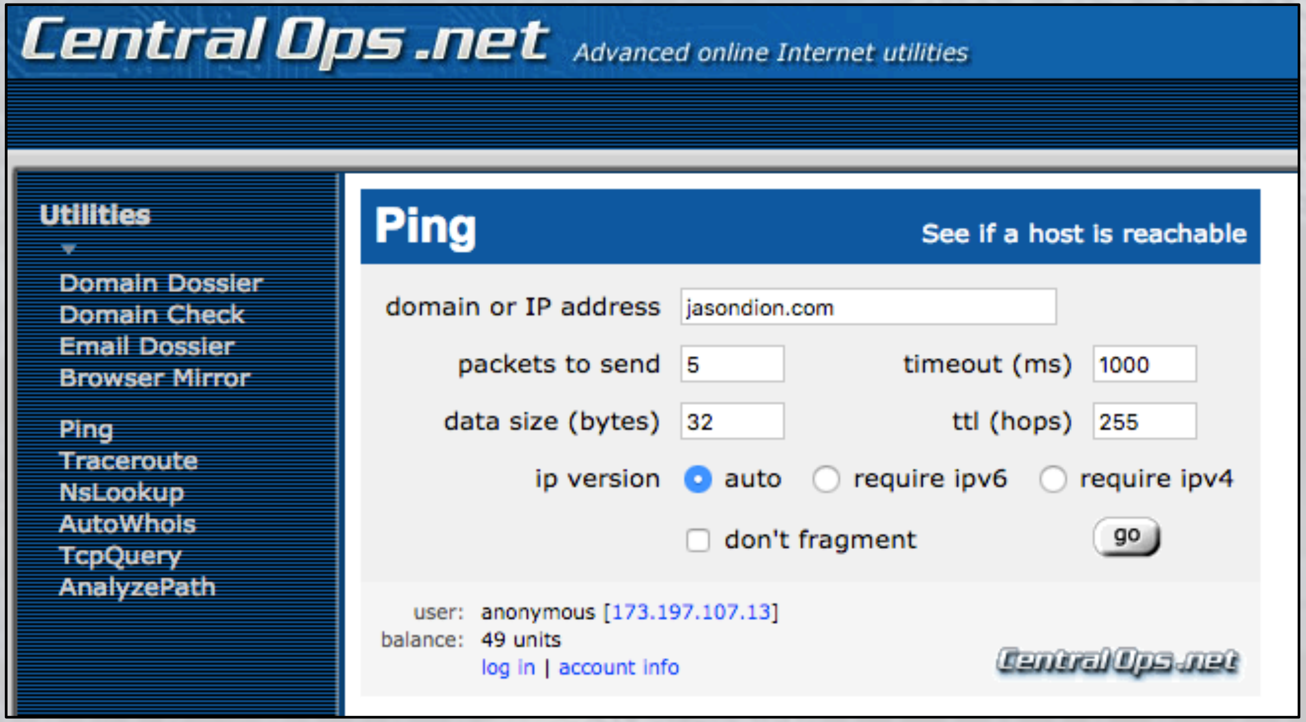
```
oot@kali:~# ping -c 6 jasondion.com
ING jasondion.com (50.87.237.193) 56(84) bytes of data.
4 bytes from 50-87-237-193.unifiedlayer.com (50.87.237.193): icmp_seq=1 ttl=63 time=99.8 ms
4 bytes from 50-87-237-193.unifiedlayer.com (50.87.237.193): icmp_seq=2 ttl=63 time=98.2 ms
4 bytes from 50-87-237-193.unifiedlayer.com (50.87.237.193): icmp_seq=3 ttl=63 time=96.8 ms
4 bytes from 50-87-237-193.unifiedlayer.com (50.87.237.193): icmp_seq=4 ttl=63 time=95.1 ms
4 bytes from 50-87-237-193.unifiedlayer.com (50.87.237.193): icmp_seq=5 ttl=63 time=103 ms
4 bytes from 50-87-237-193.unifiedlayer.com (50.87.237.193): icmp_seq=6 ttl=63 time=103 ms

-- jasondion.com ping statistics ---
 packets transmitted, 6 received, 0% packet loss, time 5009ms
tt min/avg/max/mdev = 95.114/99.593/103.885/3.279 ms
oot@kali:~# 
```

ping



```
root@kali:~# ping -c 6 jasondion.com
PING jasondion.com (50.87.237.193) 56(84) bytes of data.
64 bytes from 50-87-237-193.unifiedlayer.com (50.87.237.193): icmp_seq=1 ttl=63 time=99.8 ms
64 bytes from 50-87-237-193.unifiedlayer.com (50.87.237.193): icmp_seq=2 ttl=63 time=98.2 ms
64 bytes from 50-87-237-193.unifiedlayer.com (50.87.237.193): icmp_seq=3 ttl=63 time=96.8 ms
64 bytes from 50-87-237-193.unifiedlayer.com (50.87.237.193): icmp_seq=4 ttl=63 time=95.1 ms
64 bytes from 50-87-237-193.unifiedlayer.com (50.87.237.193): icmp_seq=5 ttl=63 time=103 ms
64 bytes from 50-87-237-193.unifiedlayer.com (50.87.237.193): icmp_seq=6 ttl=63 time=103 ms

--- jasondion.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 95.114/99.593/103.885/3.279 ms
root@kali:~# 
```

ping



Ping

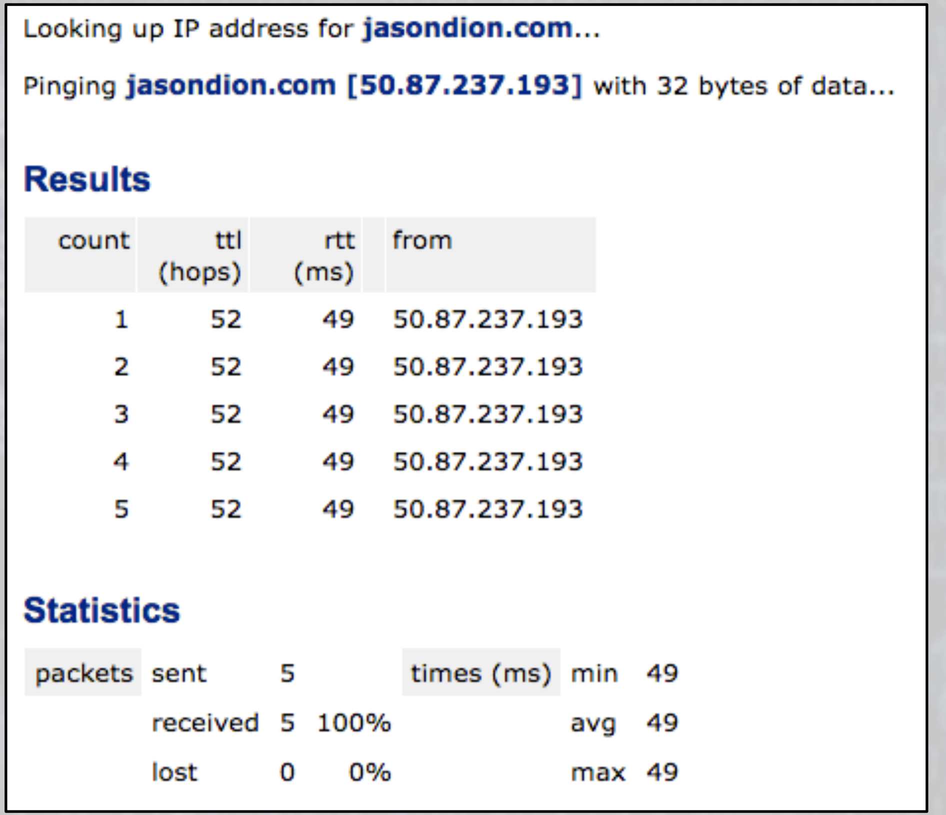
See if a host is reachable

domain or IP address	jasondion.com		
packets to send	5	timeout (ms)	1000
data size (bytes)	32	ttl (hops)	255

ip version ● auto ○ require ipv6 ○ require ipv4

□ don't fragment

user: anonymous [173.197.107.13]
balance: 49 units



Looking up IP address for **jasondion.com**...

Pinging **jasondion.com [50.87.237.193]** with 32 bytes of data...

Results

count	ttl (hops)	rtt (ms)	from
1	52	49	50.87.237.193
2	52	49	50.87.237.193
3	52	49	50.87.237.193
4	52	49	50.87.237.193
5	52	49	50.87.237.193

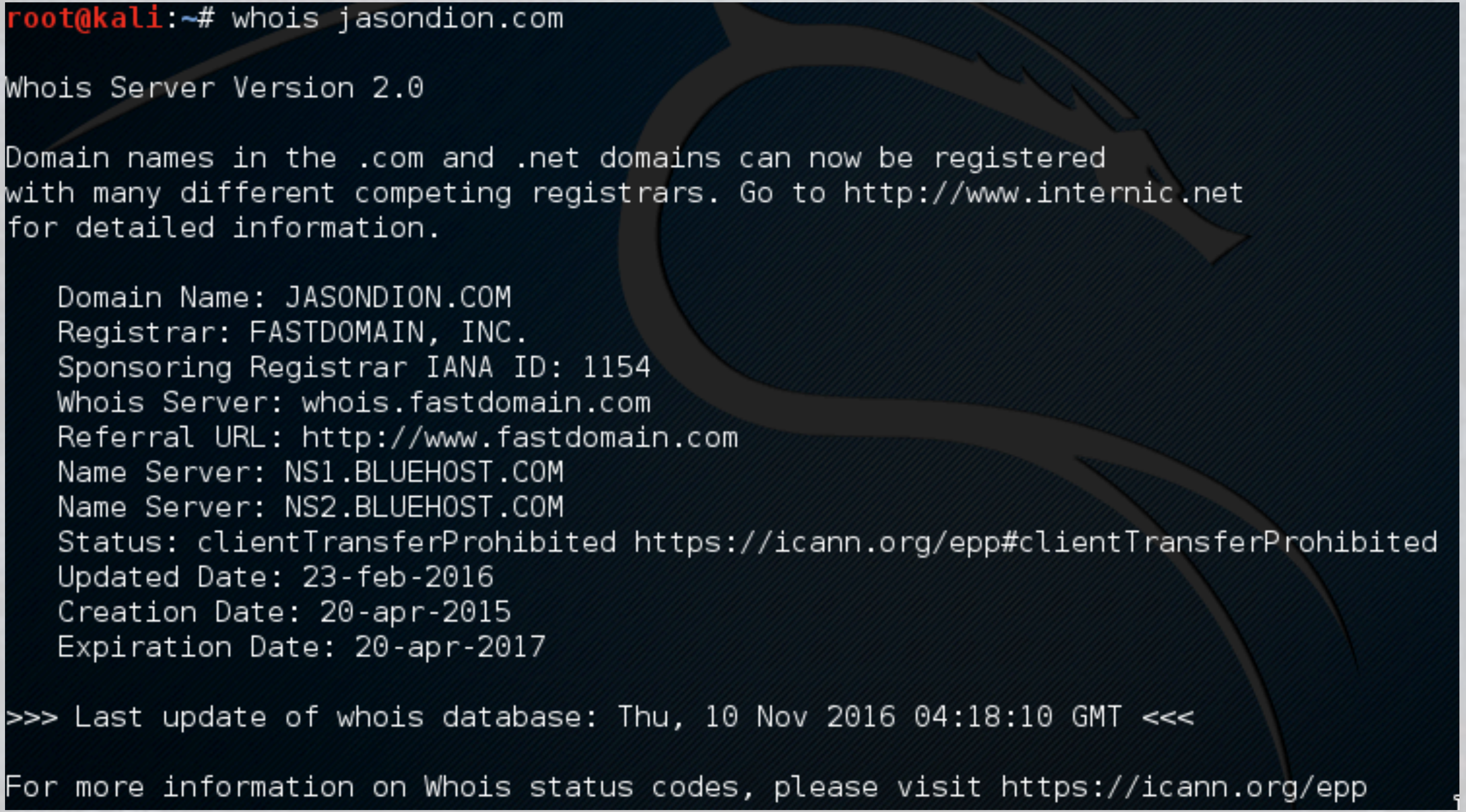
Statistics

packets	sent	5		times (ms)	min	49
	received	5	100%		avg	49
	lost	0	0%		max	49

whois

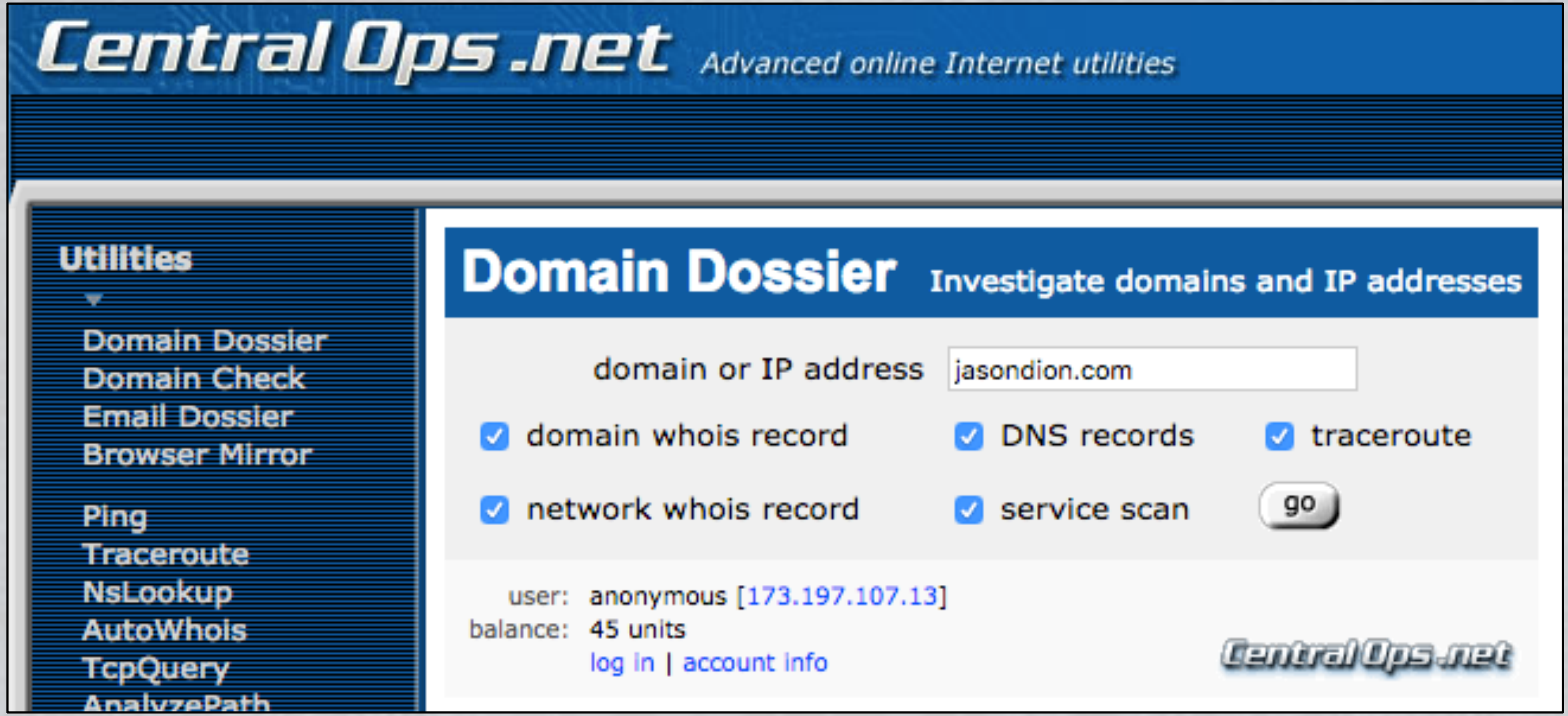
- Provides information on the owner of a domain name
- Can provide:
  - Server addresses
  - Owner’s names
  - Owner’s addresses
  - Owner’s phone numbers
- Can help to develop a successful social engineering attack against the target

whois



```
root@kali:~# whois jasondion.com

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: JASONDION.COM
   Registrar: FASTDOMAIN, INC.
   Sponsoring Registrar IANA ID: 1154
   Whois Server: whois.fastdomain.com
   Referral URL: http://www.fastdomain.com
   Name Server: NS1.BLUEHOST.COM
   Name Server: NS2.BLUEHOST.COM
   Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Updated Date: 23-feb-2016
   Creation Date: 20-apr-2015
   Expiration Date: 20-apr-2017

>>> Last update of whois database: Thu, 10 Nov 2016 04:18:10 GMT <<<

For more information on Whois status codes, please visit https://icann.org/epp
```

Domain Dossier



Domain Dossier Investigate domains and IP addresses

domain or IP address: jasondion.com

☑ domain whois record ☑ DNS records ☑ traceroute

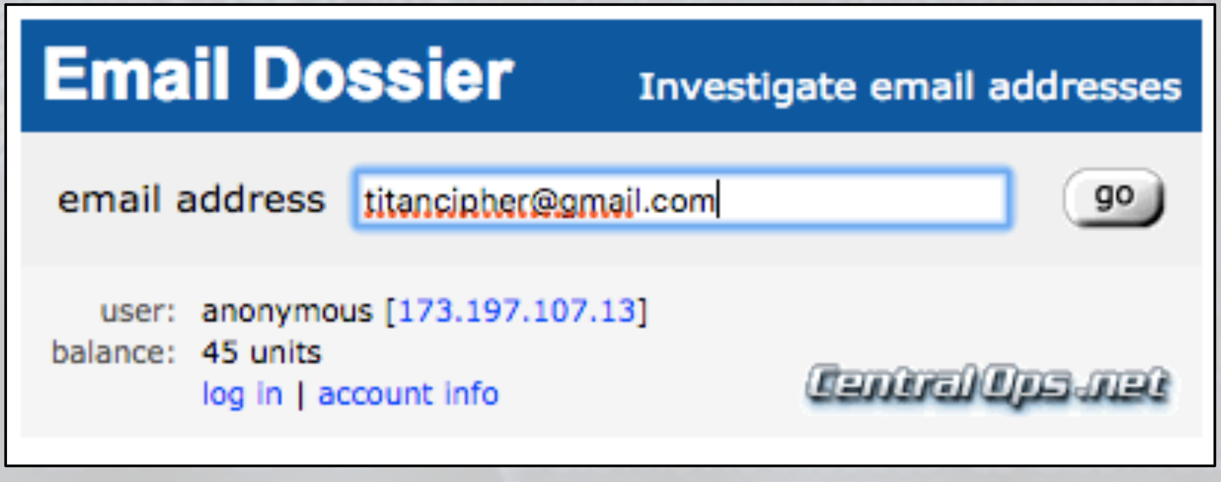
☑ network whois record ☑ service scan

user: anonymous [173.197.107.13]
balance: 45 units

- Runs the tools from the CentralOps.net server
- Adds to your anonymity during the reconnaissance phase

Email Dossier

- Email Dossier is a tool that provides:
  - Email address validation
  - MX records
    - Email server addresses
    - Email server IP addresses
    - Server precendence
  - SMTP connection log



Email Dossier Investigate email addresses

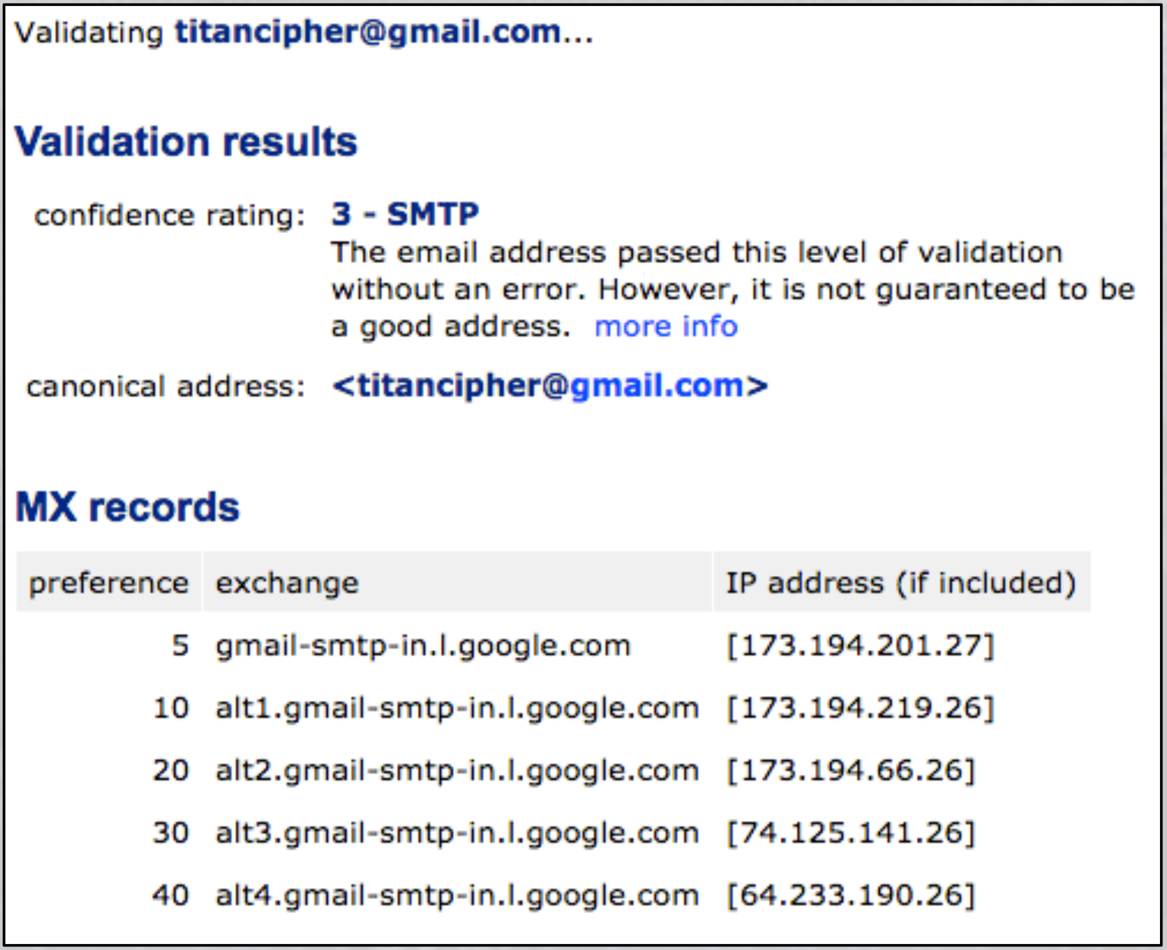
email address: titancipher@gmail.com

user: anonymous [173.197.107.13]
balance: 45 units

- Runs the tools from the CentralOps.net server

- Adds to your anonymity during the reconnaissance phase

Email Dossier



Validating **titancipher@gmail.com**...

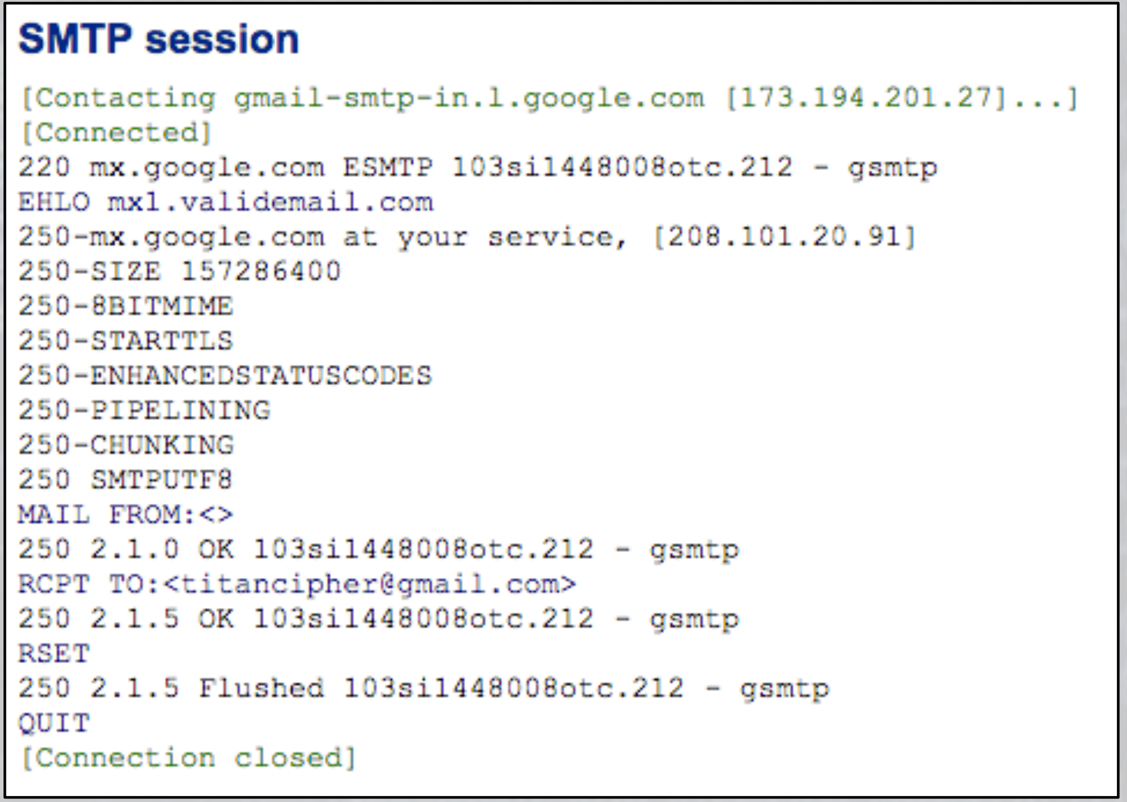
Validation results

confidence rating: **3 - SMTP**
The email address passed this level of validation without an error. However, it is not guaranteed to be a good address. more info

canonical address: **<titancipher@gmail.com>**

MX records

preference	exchange	IP address (if included)
5	gmail-smtp-in.l.google.com	[173.194.201.27]
10	alt1.gmail-smtp-in.l.google.com	[173.194.219.26]
20	alt2.gmail-smtp-in.l.google.com	[173.194.66.26]
30	alt3.gmail-smtp-in.l.google.com	[74.125.141.26]
40	alt4.gmail-smtp-in.l.google.com	[64.233.190.26]



SMTP session

```
[Contacting gmail-smtp-in.l.google.com [173.194.201.27]...]
[Connected]
220 mx.google.com ESMTP 103si1448008otc.212 - gsmtp
EHLO mx1.validemail.com
250-mx.google.com at your service, [208.101.20.91]
250-SIZE 157286400
250-8BITMIME
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-CHUNKING
250 SMTPUTF8
MAIL FROM:<>
250 2.1.0 OK 103si1448008otc.212 - gsmtp
RCPT TO:<titancipher@gmail.com>
250 2.1.5 OK 103si1448008otc.212 - gsmtp
RSET
250 2.1.5 Flushed 103si1448008otc.212 - gsmtp
QUIT
[Connection closed]
```

Google

- Excellent resource to find open-source information

- Search press releases, corporate websites, and everything else at once

- Learn some advanced Google searching methods to be efficient

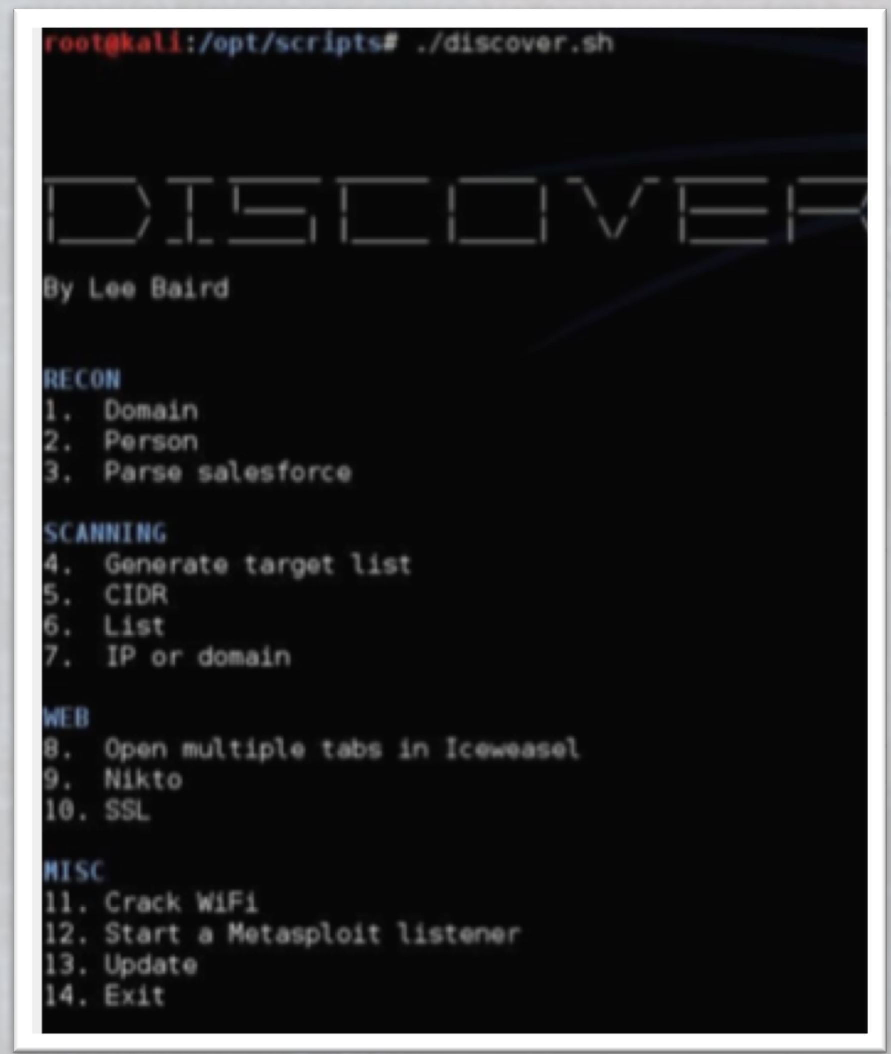
- Numerous books have been written about *Google Hacking*

Social Media

- Treasure trove of information
  - Facebook
  - LinkedIn
  - Google+
  - Twitter
  - Pinterst
  - Tumblr
  - ...and more

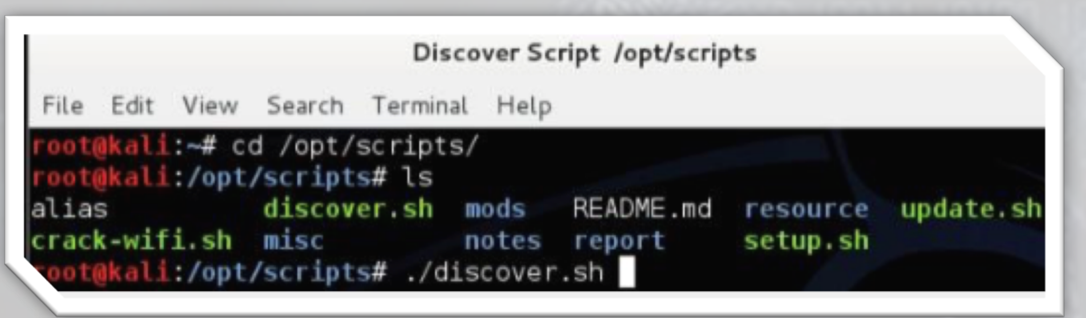
- Useful in preparing for social engineering or spearphishing campaigns against employees

Discover



```
root@kali:/opt/scripts# ./discover.sh

By Lee Baird

RECON
1.  Domain
2.  Person
3.  Parse salesforce

SCANNING
4.  Generate target list
5.  CIDR
6.  List
7.  IP or domain

WEB
8.  Open multiple tabs in Iceweasel
9.  Nikto
10. SSL

MISC
11. Crack WiFi
12. Start a Metasploit listener
13. Update
14. Exit
```

- Discover is a script written by Lee Baird
- Combines many information gathering tools within a single script
- Stored in /opt/scripts in Kali Linux
- Run discover.sh to start the script

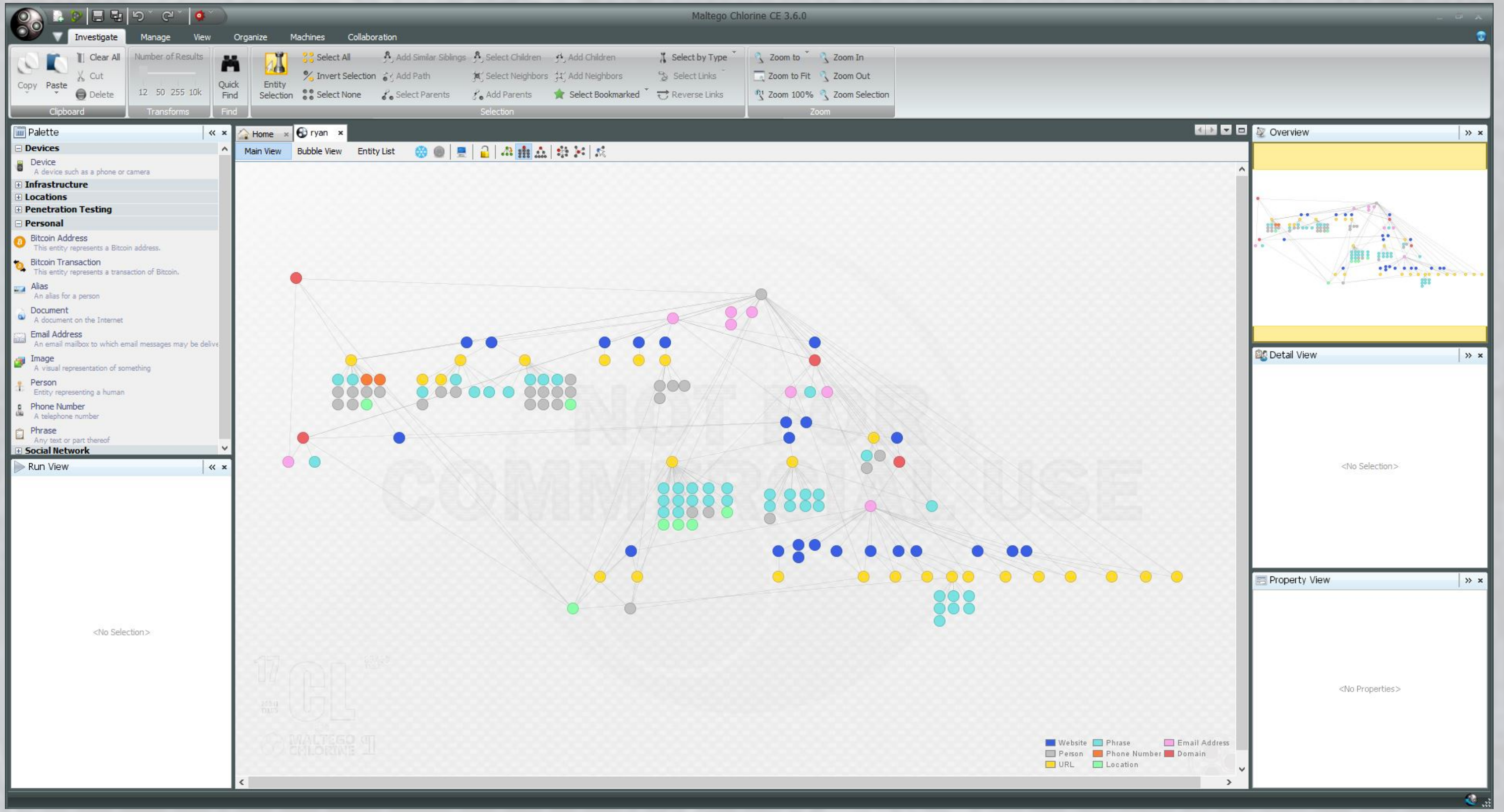


Discover Script /opt/scripts

```
root@kali:~# cd /opt/scripts/
root@kali:/opt/scripts# ls
alias         discover.sh  mods   README.md  resource  update.sh
crack-wifi.sh misc         notes  report     setup.sh
root@kali:/opt/scripts# ./discover.sh
```

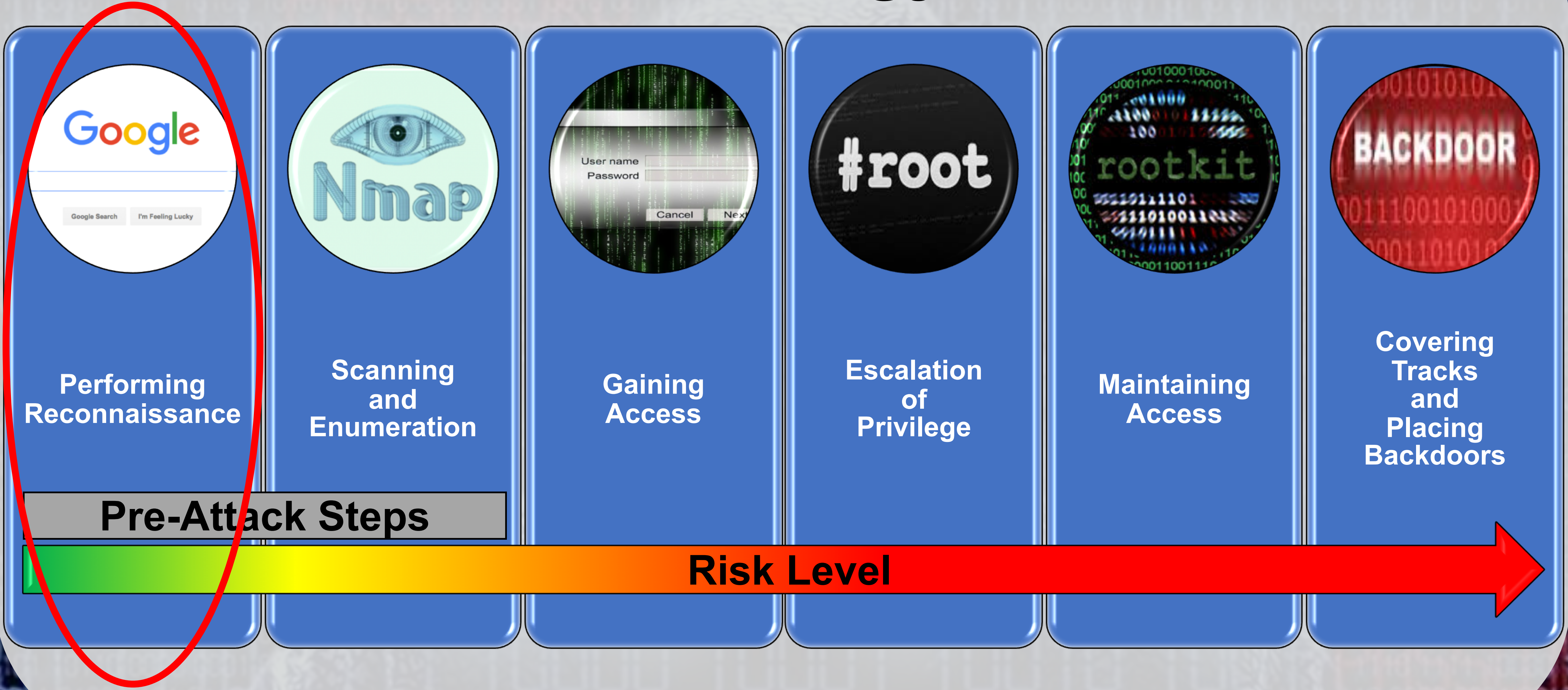
Maltego

- Tool to enumerate
  - DNS
  - Whois
  - Network blocks
  - IP addresses
  - Target individuals
    - Emails
    - Websites
    - Social networks
    - Phone numbers



- Visually depicts the relationships between people, information, and the networks they utilize

Attacker's Methodology



Performing Reconnaissance

Scanning and Enumeration

Gaining Access

Escalation of Privilege

Maintaining Access

Covering Tracks and Placing Backdoors

Pre-Attack Steps

Risk Level

Putting It All Together…

- At this point, you should have collected examples of emails, names, phone numbers, servers addresses, documents, presentations, and more.

- Use the emails to draft potential spearphishing emails to be more realistic
  - Use target's PDF, Word, Excel, and PowerPoint files to embed malware
  - Use real employee names, positions, and writing styles to mimic real email traffic

- Use domain names to buy similar ones for squatting
  - If you are targeting titancipher.com, buy titancypher.com
  - Make the site look as close to the original as possible, but host malware there

- Identify any subdomains (developer sites, mail servers, etc.) for exploitation

Reconnaissance Phase

(…I can see you but you can’t see me)