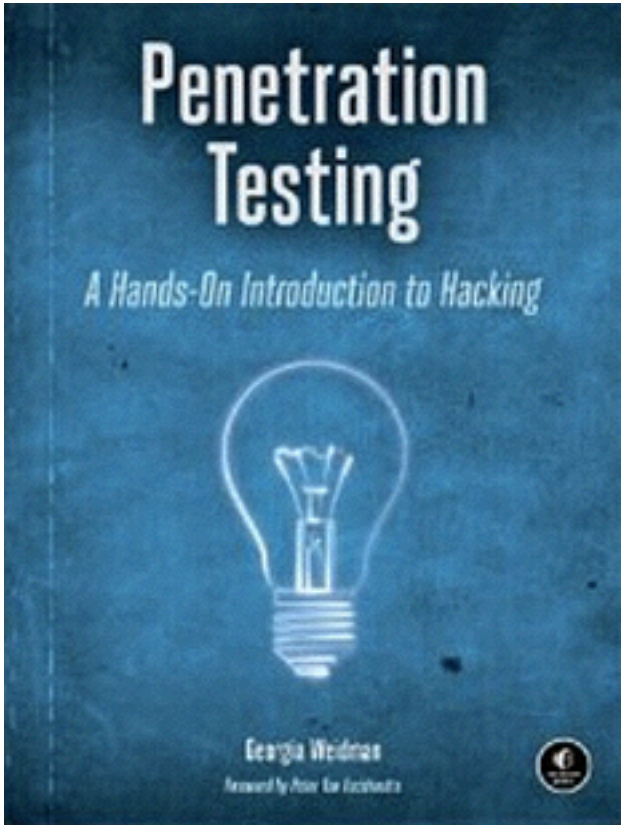
CNIT 124: Advanced Ethical Hacking



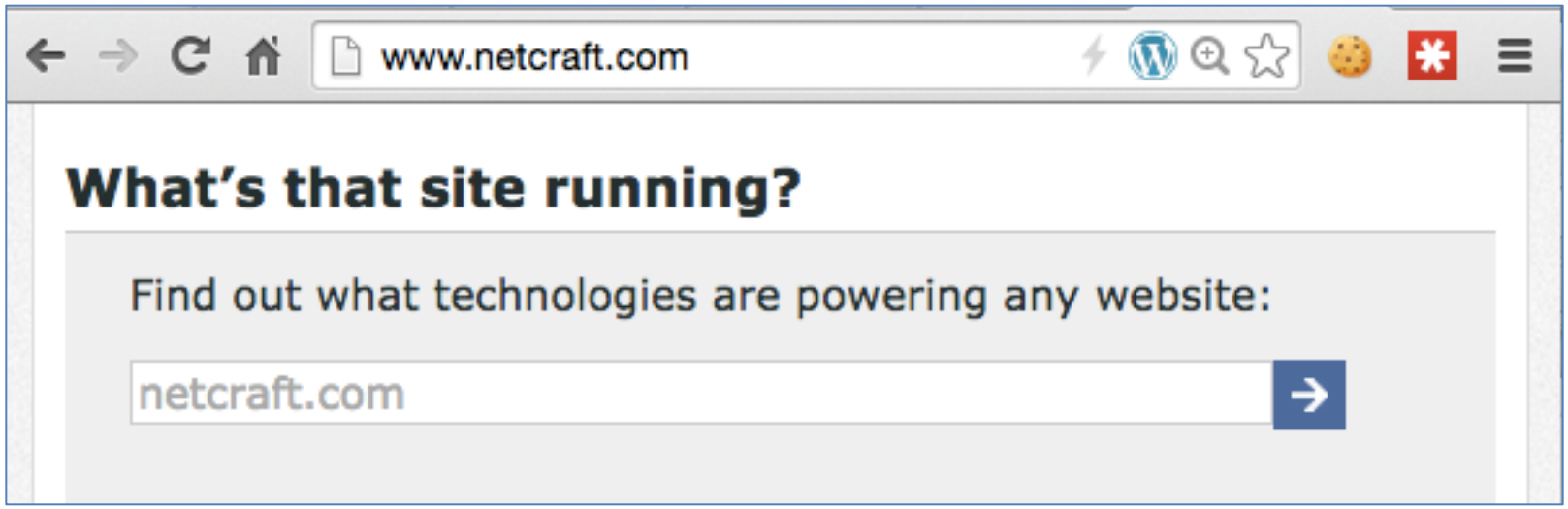
Ch 5: Information Gathering

OSINT
Open Source Intelligence

Useful Info for a Pentest

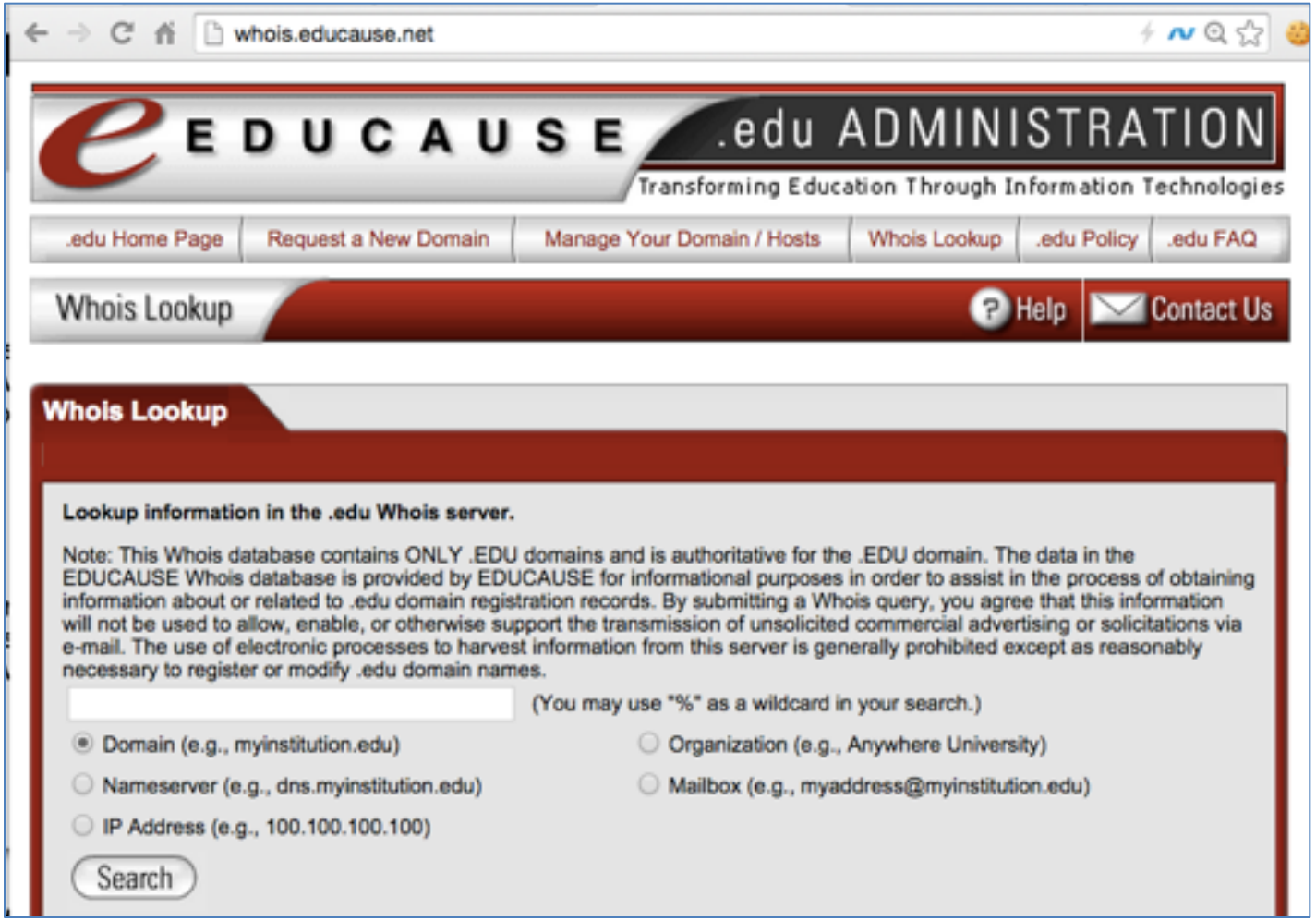
- Employees who talk too much
  - Twitter, Facebook, etc.
- Archived listservs may have technical questions
- What software and hardware are they using?
  - Defenses such as firewalls
  - Security problems
  - Extra systems like ActiveMQ

Netcraft



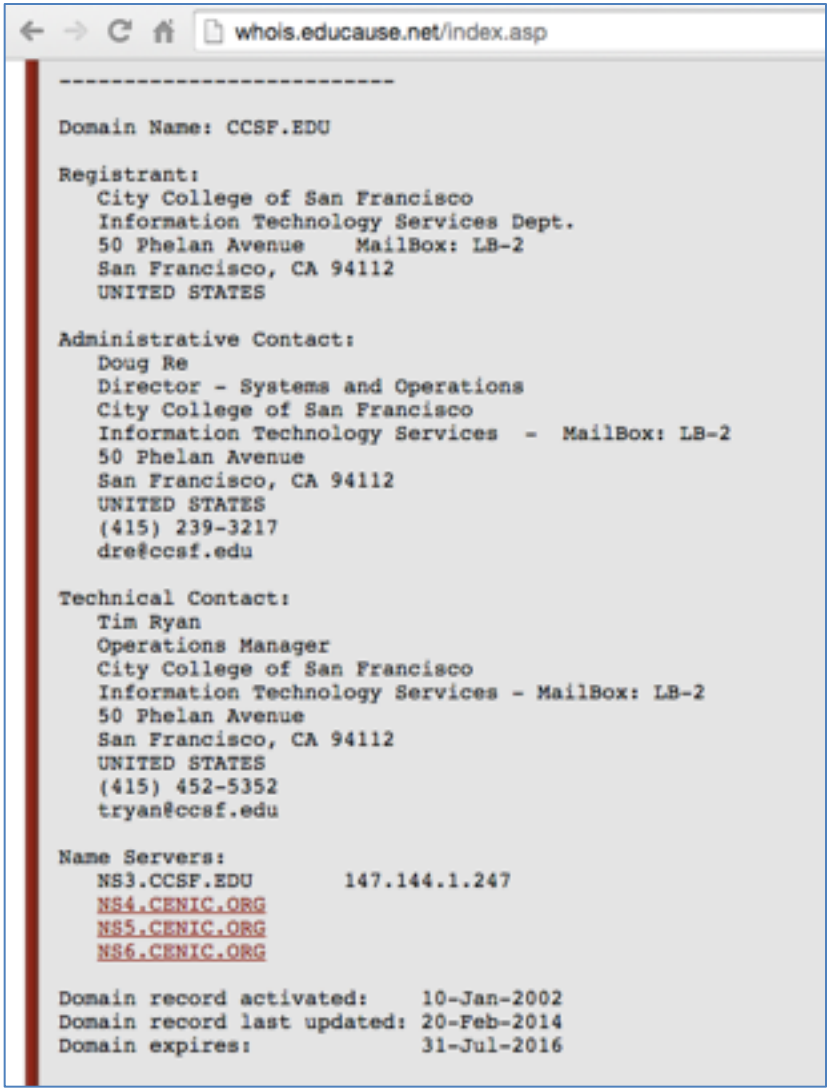
- Try ccsf.edu

Whois


whois.educause.net
EDUCAUSE
.edu ADMINISTRATION
Transforming Education Through Information Technologies
.edu Home Page
Request a New Domain
Manage Your Domain / Hosts
Whois Lookup
.edu Policy
.edu FAQ
Whois Lookup
Help
Contact Us
Whois Lookup
Lookup information in the .edu Whois server.
Note: This Whois database contains ONLY .EDU domains and is authoritative for the .EDU domain. The data in the EDUCAUSE Whois database is provided by EDUCAUSE for informational purposes in order to assist in the process of obtaining information about or related to .edu domain registration records. By submitting a Whois query, you agree that this information will not be used to allow, enable, or otherwise support the transmission of unsolicited commercial advertising or solicitations via e-mail. The use of electronic processes to harvest information from this server is generally prohibited except as reasonably necessary to register or modify .edu domain names.
(You may use "%" as a wildcard in your search.)
Domain (e.g., myinstitution.edu)
Organization (e.g., Anywhere University)
Nameserver (e.g., dns.myinstitution.edu)
Mailbox (e.g., myaddress@myinstitution.edu)
IP Address (e.g., 100.100.100.100)
Search

CCSF.EDU

- Normal record
- Informative
- Compare to kittenwar.com
- Privacy protections



Whois Limitations

- Data can be fake or concealed
- "whois microsoft.com" has a strange result (NSFW) because it searches the whole FQDN, so people have added joke records
  - Seems to no longer work as of 9-16-17

Whois Limitations

```
. . . . . .  sambowne Wed Sep 16 10:24:46
axfr $whois microsoft.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.

MICROSOFT.COM.ARE.[redacted].NET.NS-NOT-IN-SERVICE.COM
MICROSOFT.COM.CAN.GO.[redacted].ITSELF.AT.SECZY.COM
MICROSOFT.COM.EENGURRA.COM
MICROSOFT.COM.FILLS.ME.WITH.BELLIGERENCE.NET
MICROSOFT.COM.HAS.A.PRESENT.COMING.FROM.HUGHESMISSILES.COM
MICROSOFT.COM.IS.A.MESS.TIMPORTER.CO.UK
MICROSOFT.COM.IS.A.STEAMING.HEAP.OF.[redacted].NET
MICROSOFT.COM.IS.IN.BED.WITH.CURTYV.COM
MICROSOFT.COM.IS.NICE.WHEN.TOASTED.COMKAL.NET
MICROSOFT.COM.IS.NOT.HOSTED.BY.ACTIVEDOMAINDNS.NET
MICROSOFT.COM.IS.NOT.YEPPA.ORG
MICROSOFT.COM.LIVES.AT.SHAUNEWING.COM
MICROSOFT.COM.LOVES.ME.KOSMAL.NET
MICROSOFT.COM.MAKES.RICKARD.DRINK.SAMBUCA.0800CARRENTAL.COM
MICROSOFT.COM.MATCHES.THIS.STRING.AT.KEYSIGNERS.COM
```

DNS Queries

- dig samsclass.info
- dig samsclass.info aaaa
- dig samsclass.info ns
- dig samsclass.info soa
- dig samsclass.info any

DNS Lookup Type	Description	Function
A	IPv4 address record	Returns a 32-bit IP address, which typically maps a domain's hostname to an IP address, but also used for DNSBLs and storing subnet masks
AAAA	IPv6 address record	Returns a 128-bit IP address that maps a domain's hostname to an IP address
MX	Mail exchange record	Maps a domain name to a list of message transfer agents for that domain
NS	Name server record	Delegates a DNS zone to use the specified authoritative name servers
PTR	Pointer record	Pointer to a canonical name that returns the name only and is used for implementing reverse DNS lookups
SOA	Start of authority record	Specifies authoritative information about a DNS zone, including the primary name server, the email of the domain administrator, the domain serial number, and several timers relating to refreshing the zone
SRV	Service locator	Generalized service location record, used for newer protocols instead of creating protocol-specific records such as MX
TXT	Text record	Carries extra data, sometimes human-readable, most of the time machine-readable such as opportunistic encryption, DomainKeys, DNS-SD, etc.

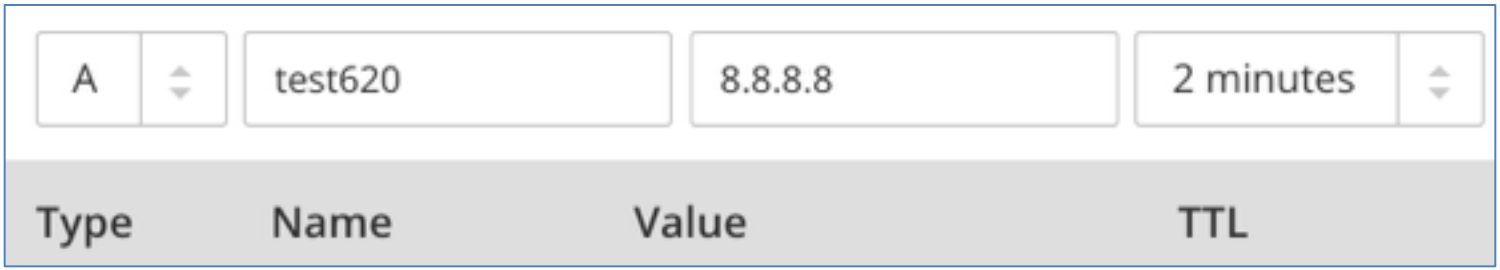
- Link Ch 5a

Dig at a specific server

- dig samsclass.info any
  - 10 records
- dig @8.8.8.8 samsclass.info any
  - 18 records
- dig @coco.ns.cloudflare.com samsclass.info any
  - 10 records

DNS Cache Snooping Demo

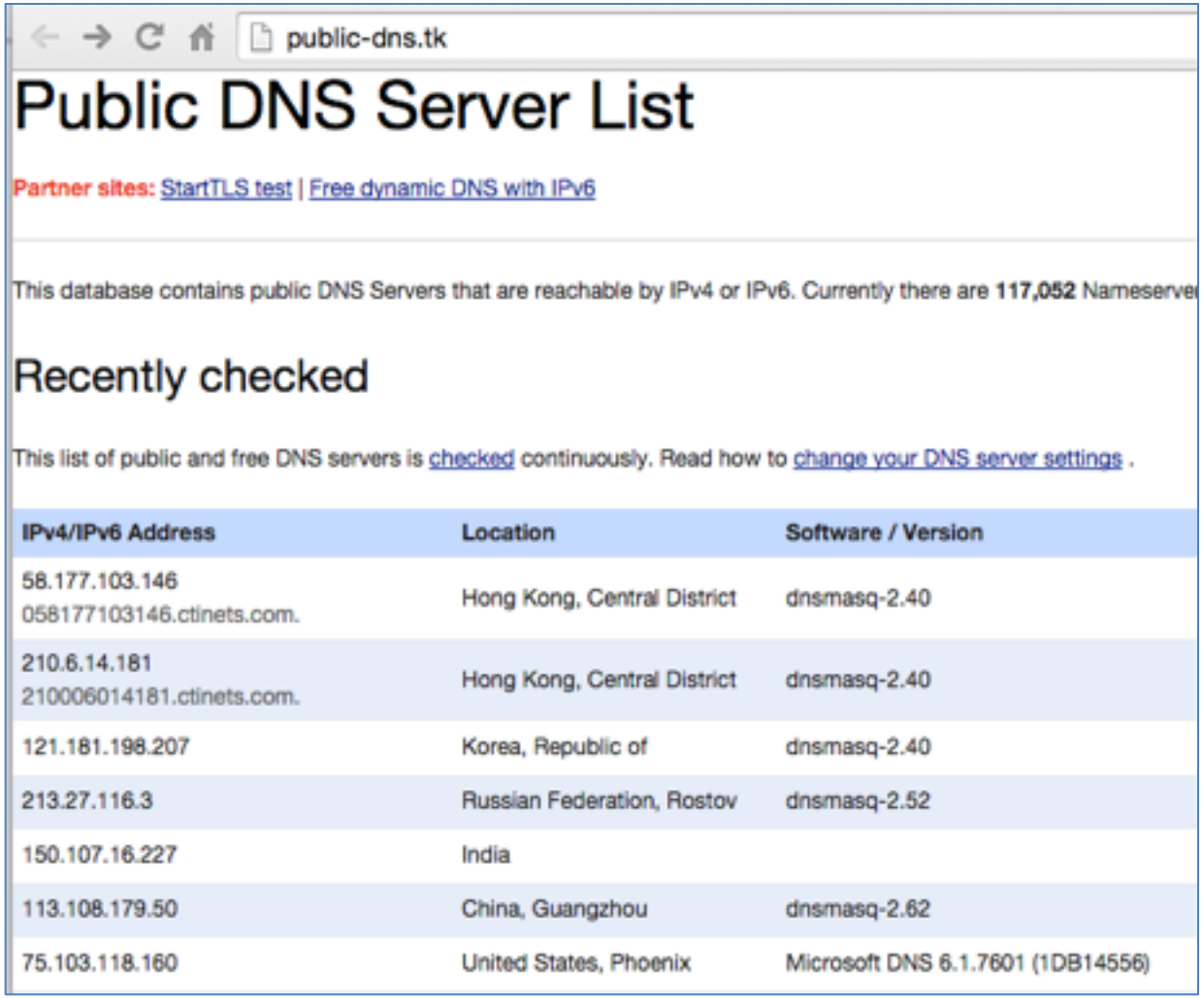
- Make a new DNS record



- dig +norecurse @109.69.8.51 test360.samsclass.info
  - Shows record, if it's in the cache
- dig @109.69.8.51 test360.samsclass.info
  - Caches record

Find a Public Resolver

- Link Ch 5d



Nonrecursive Query

- Server has no data in its cache
- Doesn't ask other servers (nonrecursive)
- Finds no answer
  - Command works the same way on Kali Linux and Mac OS X

```
. . . . . . . . . sambowne Wed Sep 16 08:34:48
~ $dig @75.103.118.160 a.samsclass.info +norecurse +noall +answer

; <<>> DiG 9.8.3-P1 <<>> @75.103.118.160 a.samsclass.info +norecurse +noall +answer
; (1 server found)
;; global options: +cmd
```

Recursive Query

- DNS server asks other servers and finds the record
- Note its TTL starts at 3600 seconds

```
.  .  .  .  .  .  .  .  .  sambowne Wed Sep 16 08:35:11
~ $dig @75.103.118.160 a.samsclass.info +recurse +noall +answer

; <<>> DiG 9.8.3-P1 <<>> @75.103.118.160 a.samsclass.info +recurse +noall +answer
; (1 server found)
;; global options: +cmd
a.samsclass.info.       3600    IN      A       8.8.8.8
```

Nonrecursive Query

- Now the data is in the cache
- This shows that someone has resolved that site on this server recently

```
.  .  .  .  .  .  .  .  .  sambowne Wed Sep 16 08:35:26
~ $dig @75.103.118.160 a.samsclass.info +norecurse +noall +answer

; <<>> DiG 9.8.3-P1 <<>> @75.103.118.160 a.samsclass.info +norecurse +noall +answer
; (1 server found)
;; global options: +cmd
a.samsclass.info.       3593    IN      A       8.8.8.8
```

Demo: puntCAT Server

```
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @109.69.8.51 test630.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +short @109.69.8.51 test630.samsclass.info
104.28.17.29
104.28.16.29
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @109.69.8.51 test630.samsclass.info
104.28.16.29
104.28.17.29
```

- Cache Snooping works simply on a single server
- Public DNS Servers: Link Ch 5j

Demo: OpenDNS Cluster

```
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test630.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test630.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test630.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test630.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test630.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test630.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test630.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test630.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test630.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test630.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$
Sams-MacBook-Pro-3:parity sambowne$ dig +short @208.67.222.222 test630.samsclass.info
104.28.17.29
104.28.16.29
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test630.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test630.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test630.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test630.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test630.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test630.samsclass.info
104.28.16.29
104.28.17.29
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test630.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test630.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test630.samsclass.info
104.28.16.29
104.28.17.29
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test630.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test630.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test630.samsclass.info
104.28.16.29
104.28.17.29
```

- One recursive query puts it in one cache
- Cached record observed in 3/12 queries

Demo: OpenDNS Cluster

```
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test620.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test620.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test620.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test620.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test620.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test620.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test620.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test620.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test620.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test620.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$
Sams-MacBook-Pro-3:parity sambowne$
Sams-MacBook-Pro-3:parity sambowne$ dig +short @208.67.222.222 test620.samsclass.info
104.28.16.29
104.28.17.29
Sams-MacBook-Pro-3:parity sambowne$ dig +short @208.67.222.222 test620.samsclass.info
104.28.17.29
104.28.16.29
```

- Ten recursive queries puts it in more caches

Demo: OpenDNS Cluster

```
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test620.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test620.samsclass.info
104.28.17.29
104.28.16.29
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test620.samsclass.info
104.28.16.29
104.28.17.29
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test620.samsclass.info
104.28.17.29
104.28.16.29
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test620.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test620.samsclass.info
104.28.16.29
104.28.17.29
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test620.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test620.samsclass.info
104.28.16.29
104.28.17.29
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test620.samsclass.info
Sams-MacBook-Pro-3:parity sambowne$ dig +norecurse +short @208.67.222.222 test620.samsclass.info
104.28.17.29
104.28.16.29
```

- Cached record observed in 6/10 queries

Watching TTL Count Down

```
. . . . . . . . . sambowne Wed Sep 16 08:35:26
~ $dig @75.103.118.160 a.samsclass.info +norecurse +noall +answer

; <<>> DiG 9.8.3-P1 <<>> @75.103.118.160 a.samsclass.info +norecurse +noall +answer
; (1 server found)
;; global options: +cmd
a.samsclass.info.       3593    IN      A       8.8.8.8

. . . . . . . . . sambowne Wed Sep 16 08:35:32
~ $dig @75.103.118.160 a.samsclass.info +norecurse +noall +answer

; <<>> DiG 9.8.3-P1 <<>> @75.103.118.160 a.samsclass.info +norecurse +noall +answer
; (1 server found)
;; global options: +cmd
a.samsclass.info.       3317    IN      A       8.8.8.8

. . . . . . . . . sambowne Wed Sep 16 08:40:09
~ $dig @75.103.118.160 a.samsclass.info +norecurse +noall +answer

; <<>> DiG 9.8.3-P1 <<>> @75.103.118.160 a.samsclass.info +norecurse +noall +answer
; (1 server found)
;; global options: +cmd
a.samsclass.info.       3312    IN      A       8.8.8.8
```

Zone Transfers

- First find SOA

```
root@kali:~/127/ch4# dig zonetransfer.me soa

; <<>> DiG 9.9.5-9+deb8u2-Debian <<>> zonetransfer.me soa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47754
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0005 , udp: 4096
;; QUESTION SECTION:
;zonetransfer.me.               IN      SOA

;; ANSWER SECTION:
zonetransfer.me.        5       IN      SOA     nsztm1.digi.ninja. robin.digi.ninja. 2014101601 17280
0 900 1209600 3600
```

Performing Zone Transfer

```
root@kali:~/127/ch4# host -l zonetransfer.me nsztm1.digi.ninja
Using domain server:
Name: nsztm1.digi.ninja
Address: 81.4.108.41#53
Aliases:

zonetransfer.me has address 217.147.180.162
zonetransfer.me name server nsztm1.digi.ninja.
zonetransfer.me name server nsztm2.digi.ninja.
164.180.147.217.IN-ADDR.ARPA.zonetransfer.me domain name pointer www.zonetransfer.me.
asfdbbox.zonetransfer.me has address 127.0.0.1
canberra-office.zonetransfer.me has address 202.14.81.230
dc-office.zonetransfer.me has address 143.228.181.132
deadbeef.zonetransfer.me has IPv6 address dead:beaf::
email.zonetransfer.me has address 74.125.206.26
internal.zonetransfer.me name server intns1.zonetransfer.me.
internal.zonetransfer.me name server intns2.zonetransfer.me.
intns1.zonetransfer.me has address 167.88.42.94
intns2.zonetransfer.me has address 167.88.42.94
office.zonetransfer.me has address 4.23.39.254
ipv6actnow.org.zonetransfer.me has IPv6 address 2001:67c:2e8:11::c100:1332
owa.zonetransfer.me has address 207.46.197.32
alltcpportsopen.firewall.test.zonetransfer.me has address 127.0.0.1
vpn.zonetransfer.me has address 174.36.59.154
www.zonetransfer.me has address 217.147.180.162
root@kali:~/127/ch4#
```

University System of Georgia

- 1038 records
- Link Ch 5e

```
; <<>> DiG 9.9.5-3ubuntu0.2-Ubuntu <<>> +time=2 +tries=1 axfr armstrong.edu @ns3.usg.edu.
;; global options: +cmd
armstrong.edu.          14400   IN      SOA     infoblox01.armstrong.edu. sysadm.armstrong.edu. 2015
041302 10800 3600 604800 3600
armstrong.edu.          14400   IN      A       54.172.237.58
armstrong.edu.          14400   IN      TXT     "google-site-verification=grTKmlEGPbY3FHjTbnYIClmoRo
0rsJWPXtHshA7b_WI"
armstrong.edu.          14400   IN      TXT     "v=spf1 include:_spf.google.com ip4:130.254.32.70 ip
4:130.254.32.71 ip4:130.254.32.72 ip4:130.254.32.73 ip4:130.254.32.74 a:smtp.notification.com a:smtp
1.notification.com ~all"
armstrong.edu.          14400   IN      MX      10 aspmx.l.google.com.
armstrong.edu.          14400   IN      MX      20 alt1.aspmx.l.google.com.
armstrong.edu.          14400   IN      MX      20 alt2.aspmx.l.google.com.
armstrong.edu.          14400   IN      MX      30 aspmx2.googlemail.com.
armstrong.edu.          14400   IN      MX      30 aspmx3.googlemail.com.
armstrong.edu.          14400   IN      NS      ns1.usg.edu.
armstrong.edu.          14400   IN      NS      ns2.usg.edu.
armstrong.edu.          14400   IN      NS      ns3.usg.edu.
armstrong.edu.          14400   IN      NS      ns4.usg.edu.
armstrong.edu.          14400   IN      NS      infoblox01.armstrong.edu.
armstrong.edu.          14400   IN      NS      infoblox02.armstrong.edu.
armstrong.edu.          14400   IN      NS      infoblox03.armstrong.edu.
5k.armstrong.edu.       14400   IN      CNAME   web02.armstrong.edu.
www.5k.armstrong.edu.   14400   IN      CNAME   web02.armstrong.edu.
75.armstrong.edu.       14400   IN      CNAME   web02.armstrong.edu.
www.75.armstrong.edu.   14400   IN      CNAME   web02.armstrong.edu.
aasu.armstrong.edu.     14400   IN      CNAME   home.armstrong.edu.
aasu-132-11.armstrong.edu. 14400 IN     CNAME   llp-xerox.armstrong.edu.
aasu-133-13.armstrong.edu. 14400 IN     CNAME   annex3-hr-xerox.armstrong.edu.
aasu-136-11.armstrong.edu. 14400 IN     CNAME   medical-lab-sciences-xerox.armstrong.edu.
aasu-136-15.armstrong.edu. 14400 IN     CNAME   central-receiving-xerox-8900.armstrong.edu.
aasu-136-19.armstrong.edu. 14400 IN     CNAME   armc226-xerox-wc5745.armstrong.edu.
aasu-136-20.armstrong.edu. 14400 IN     CNAME   armc212-xerox5135.armstrong.edu.
aasu-136-26.armstrong.edu. 14400 IN     CNAME   military-science-xerox.armstrong.edu.
```

Fierce DNS Scanner

- included in Kali
- Attempts a zone transfer
- Then brute-forces domain names

```
root@kali:~/124/p4# fierce -dns samsclass.info
DNS Servers for samsclass.info:
        coco.ns.cloudflare.com
        tom.ns.cloudflare.com

Trying zone transfer first...
        Testing coco.ns.cloudflare.com
                Request timed out or transfer not allowed.
        Testing tom.ns.cloudflare.com
                Request timed out or transfer not allowed.

Unsuccessful in zone transfer (it was worth a shot)
Okay, trying the good old fashioned way... brute force

Checking for wildcard DNS...
Nope. Good.
Now performing 2280 test(s)...
8.8.8.8 a.samsclass.info
8.8.4.4 b.samsclass.info
```

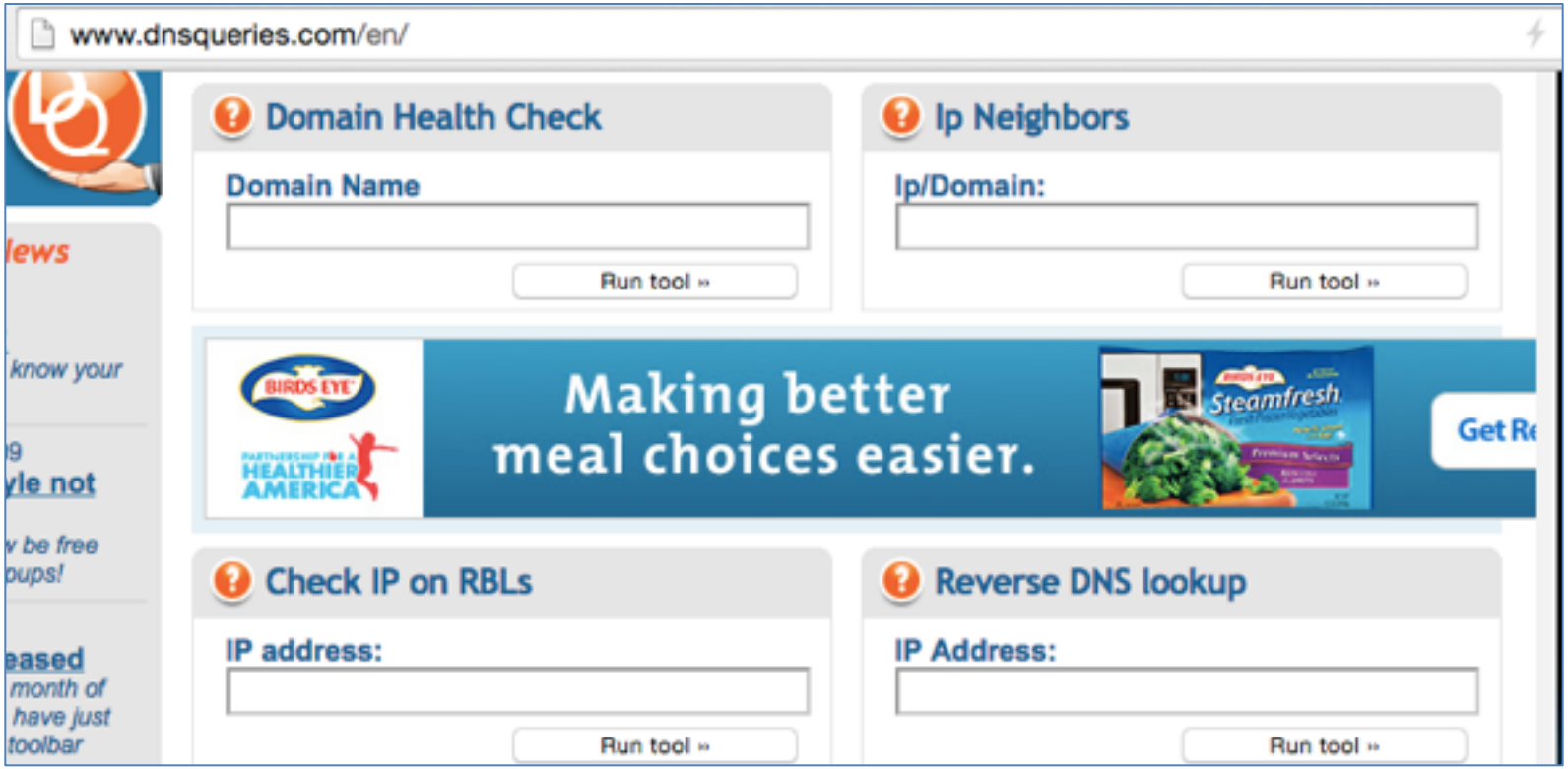
Fierce on Zonetransfer.me

```
root@kali:~/127/p6x-1# fierce -dns zonetransfer.me
DNS Servers for zonetransfer.me:
        nsztm1.digi.ninja
        nsztm2.digi.ninja

Trying zone transfer first...
        Testing nsztm1.digi.ninja

Whoah, it worked - misconfigured DNS server found:
zonetransfer.me.        7200    IN      SOA     nsztm1.digi.ninja. robin.digi.ninja. (
                                        2014101601      ;serial
                                        172800          ;refresh
                                        900             ;retry
                                        1209600         ;expire
                                        3600    )       ;minimum
zonetransfer.me.        300     IN      HINFO   "Casio fx-700G" "Windows XP"
zonetransfer.me.        301     IN      TXT     google-site-verification=tyP28J7JAUHA9fw2sHXMg
cCC0I6XBmmoVi04VlMewxA
zonetransfer.me.        7200    IN      MX      0 ASPMX.L.GOOGLE.COM.
zonetransfer.me.        7200    IN      MX      10 ALT1.ASPMX.L.GOOGLE.COM.
```

```
sqli.zonetransfer.me.    300     IN      TXT     "' or 1=1 --"
sshock.zonetransfer.me. 7200     IN      TXT     "() { :]}; echo ShellShocked"
staging.zonetransfer.me.         7200    IN      CNAME   www.sydneyoperahouse.com.
alltcpportsopen.firewall.test.zonetransfer.me.  301     IN      A       127.0.0.1
testing.zonetransfer.me.         301     IN      CNAME   www.zonetransfer.me.
vpn.zonetransfer.me.     4000    IN      A       174.36.59.154
www.zonetransfer.me.     7200    IN      A       217.147.180.162
xss.zonetransfer.me.     300     IN      TXT     '><script>alert\('Boo'\)</script>

There isn't much point continuing, you have everything.
Have a nice day.
Exiting...
root@kali:~/127/p6x-1#
```

DNSqueries.com

- Link Ch 5h




Kahoot!

Searching for Email Addresses

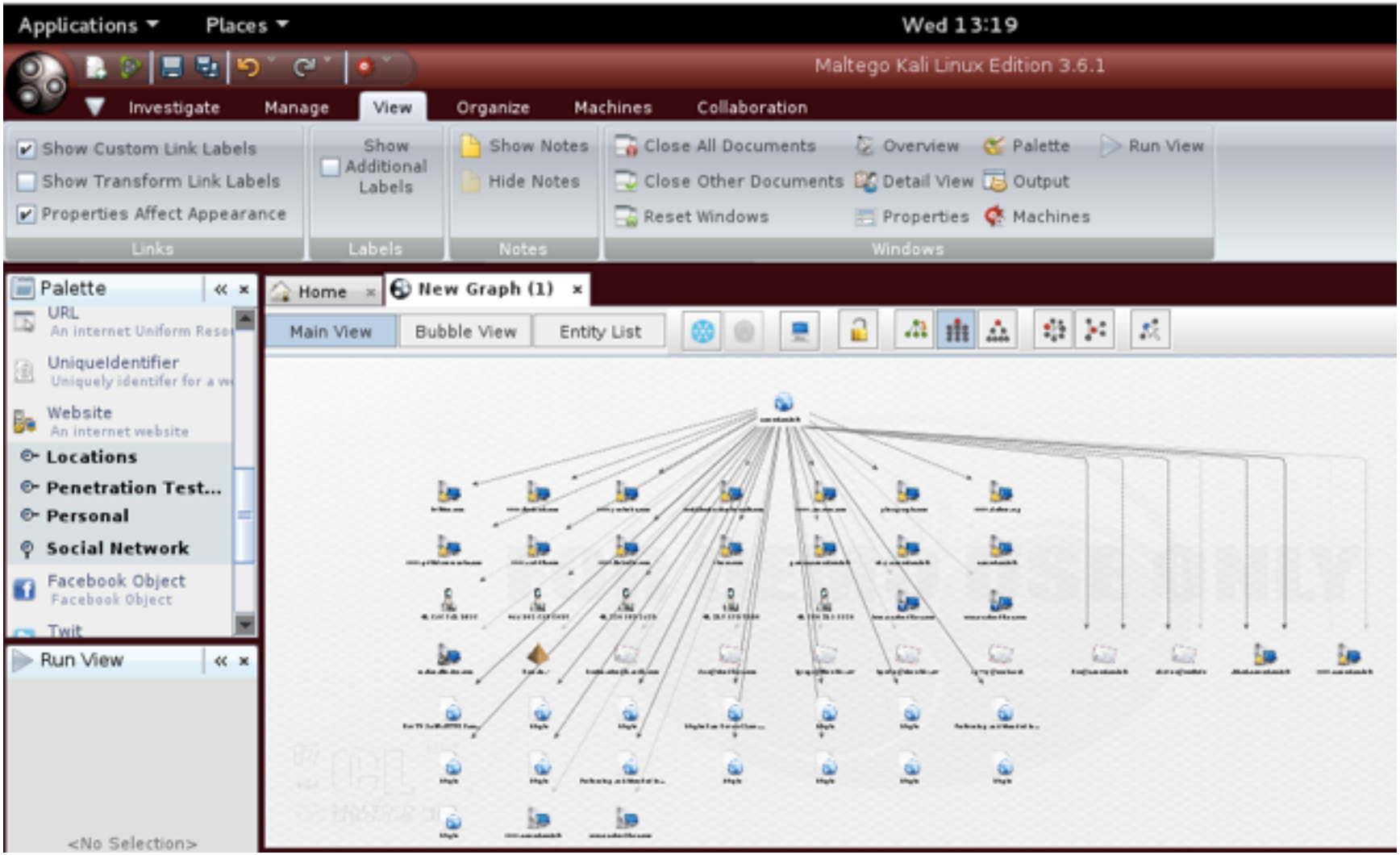
theHarvester

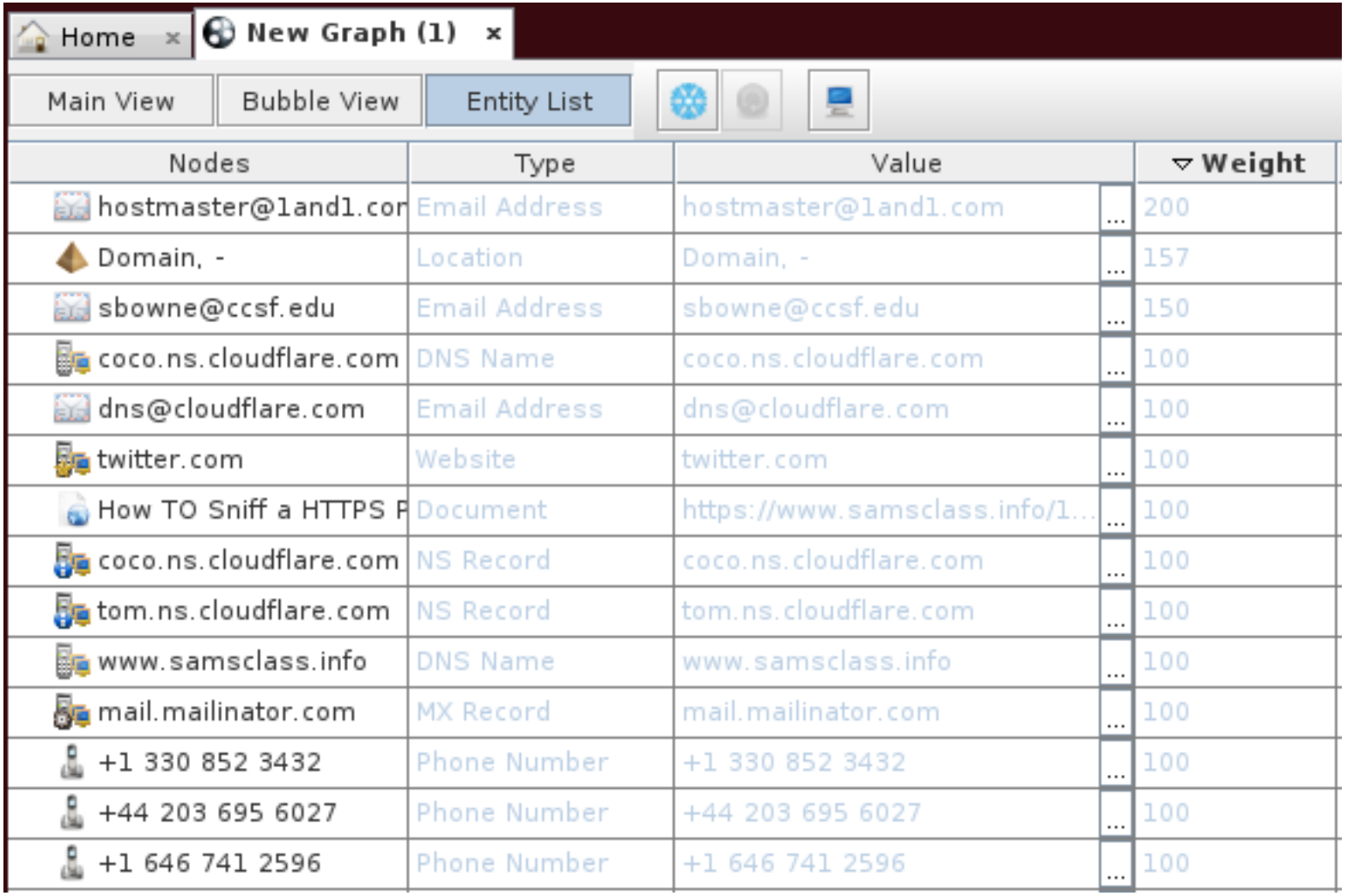
```
root@kali:~/127/p6x-1# theharvester -d edge-security.com -b all
```

- Searches Google. Bing, and other sources for email addresses
- Also finds sites hosted at the same IP

```
Full harvest..
[-] Searching in Google..
        Searching 0 results...
        Searching 100 results...
[-] Searching in PGP Key server..
[-] Searching in Bing..
        Searching 50 results...
        Searching 100 results...
[-] Searching in Exalead..
        Searching 50 results...
        Searching 100 results...
        Searching 150 results...


[+] Emails found:
------------------
cmartorella@edge-security.com
xmendez@edge-security.com
@edge-security.com
cmartorella@edge-security.com
@edge-security.com
```

Maltego


Applications
Places
Wed 13:19
Maltego Kali Linux Edition 3.6.1
Investigate
Manage
View
Organize
Machines
Collaboration
Show Custom Link Labels
Show Transform Link Labels
Properties Affect Appearance
Links
Show Additional Labels
Labels
Show Notes
Hide Notes
Notes
Close All Documents
Close Other Documents
Reset Windows
Overview
Detail View
Properties
Palette
Output
Machines
Run View
Windows
Palette
URL
UniqueIdentifier
Website
An internet website
Locations
Penetration Test...
Personal
Social Network
Facebook Object
Facebook Object
Twit
Run View
<No Selection>
Home
New Graph (1)
Main View
Bubble View
Entity List


Home
New Graph (1)
Main View
Bubble View
Entity List
Nodes
Type
Value
Weight
hostmaster@1and1.cor
Email Address
hostmaster@1and1.com
200
Domain, -
Location
Domain, -
157
sbowne@ccsf.edu
Email Address
sbowne@ccsf.edu
150
coco.ns.cloudflare.com
DNS Name
coco.ns.cloudflare.com
100
dns@cloudflare.com
Email Address
dns@cloudflare.com
100
twitter.com
Website
twitter.com
100
How TO Sniff a HTTPS F
Document
https://www.samsclass.info/1...
100
coco.ns.cloudflare.com
NS Record
coco.ns.cloudflare.com
100
tom.ns.cloudflare.com
NS Record
tom.ns.cloudflare.com
100
www.samsclass.info
DNS Name
www.samsclass.info
100
mail.mailinator.com
MX Record
mail.mailinator.com
100
+1 330 852 3432
Phone Number
+1 330 852 3432
100
+44 203 695 6027
Phone Number
+44 203 695 6027
100
+1 646 741 2596
Phone Number
+1 646 741 2596
100

Port Scanning

Manual Port Scanning

- Some services show a banner as soon as a connection is made

```
root@kali:~/127/ch4# nc 192.168.119.129 25
220 WIN-JWBPPZSXEFV SMTP Server SLmail 5.5.0.4433 Ready ESMTP spoken here
^C
root@kali:~/127/ch4# nc attack.samsclass.info 22
SSH-2.0-OpenSSH_6.6p1 Ubuntu-2ubuntu1
```

- The banner could be deceptive, however
- Many services, like HTTP and DNS, don't deliver a banner so easily

Nmap SYN Scan

- -sS switch
- Sends SYN, listens for SYN/ACK
- Doesn't complete the handshake, just sends a RST

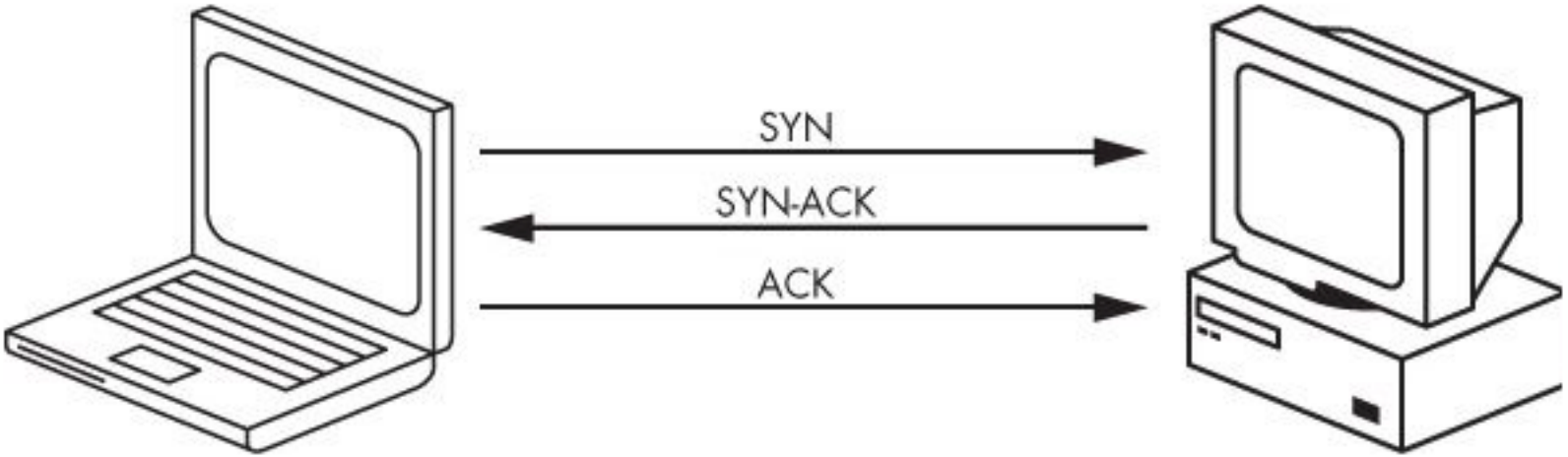


Figure 5-7. TCP three-way handshake

Nmap Scan Limitations

- Nmap is so popular, IDS and IPS systems often detect it
- They may block all results

SYN Scan of Server 2008

```
root@kali:~/127/ch4# nmap -sS 192.168.119.129

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-09-16 14:30 EDT
Nmap scan report for 192.168.119.129
Host is up (0.00035s latency).
Not shown: 981 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
79/tcp   open  finger
80/tcp   open  http
106/tcp  open  pop3pw
110/tcp  open  pop3
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1027/tcp open  IIS
1028/tcp open  unknown
1029/tcp open  ms-lsa
1030/tcp open  iad1
3306/tcp open  mysql
5357/tcp open  wsdapi
8080/tcp open  http-proxy
MAC Address: 00:0C:29:89:69:45 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 39.96 seconds
root@kali:~/127/ch4#
```

Took 40 sec.

Version Scan

- -sV switch
- Grabs banners to determine version

Version Scan of Windows 2008

```
root@kali:~/127/ch4# nmap -sV 192.168.119.129

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-09-16 14:35 EDT
Nmap scan report for 192.168.119.129
Host is up (0.00064s latency).
Not shown: 981 closed ports
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp?
25/tcp   open  smtp         SLmail smtpd 5.5.0.4433
79/tcp   open  finger       SLMail fingerd
80/tcp   open  http         Apache httpd 2.2.12 ((Win32) DAV/2 mod_ssl/2.2.12 OpenS
SL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0)
106/tcp  open  pop3pw       SLMail pop3pw
110/tcp  open  pop3         BVRP Software SLMAIL pop3d
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows 98 netbios-ssn
443/tcp  open  ssl/http     Apache httpd 2.2.12 ((Win32) DAV/2 mod_ssl/2.2.12 OpenS
SL/0.9.8k mod_autoindex_color PHP/5.3.0 mod_perl/2.0.4 Perl/v5.10.0)
445/tcp  open  microsoft-ds (primary domain: WORKGROUP)
1025/tcp open  msrpc        Microsoft Windows RPC
1026/tcp open  msrpc        Microsoft Windows RPC
1027/tcp open  msrpc        Microsoft Windows RPC
1028/tcp open  msrpc        Microsoft Windows RPC
1029/tcp open  msrpc        Microsoft Windows RPC
1030/tcp open  msrpc        Microsoft Windows RPC
3306/tcp open  mysql        MySQL (unauthorized)
5357/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8080/tcp open  http-proxy?
1 service unrecognized despite returning data. If you know the service/version, ple
ase submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-ser
```

Took 110 sec.

UDP Scans

- -sU switch
- Sends packets to commonly-used UDP ports
- Packets are valid service requests
- Servers running on default ports will reply
- Closed ports return an "ICMP Unreachable" packet
- Cannot tell an open port that doesn't reply from a filtered port

UDP Scan of Windows 2008

```
root@kali:~/127/ch4# nmap -sU 192.168.119.129

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-09-16 14:38 EDT
Nmap scan report for 192.168.119.129
Host is up (0.00052s latency).
Not shown: 991 closed ports
PORT     STATE         SERVICE
69/udp   open|filtered tftp
123/udp  open|filtered ntp
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
161/udp  open|filtered snmp
500/udp  open|filtered isakmp
3702/udp open|filtered ws-discovery
4500/udp open|filtered nat-t-ike
5355/udp open|filtered llmnr
MAC Address: 00:0C:29:89:69:45 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1211.35 seconds
root@kali:~/127/ch4#
```

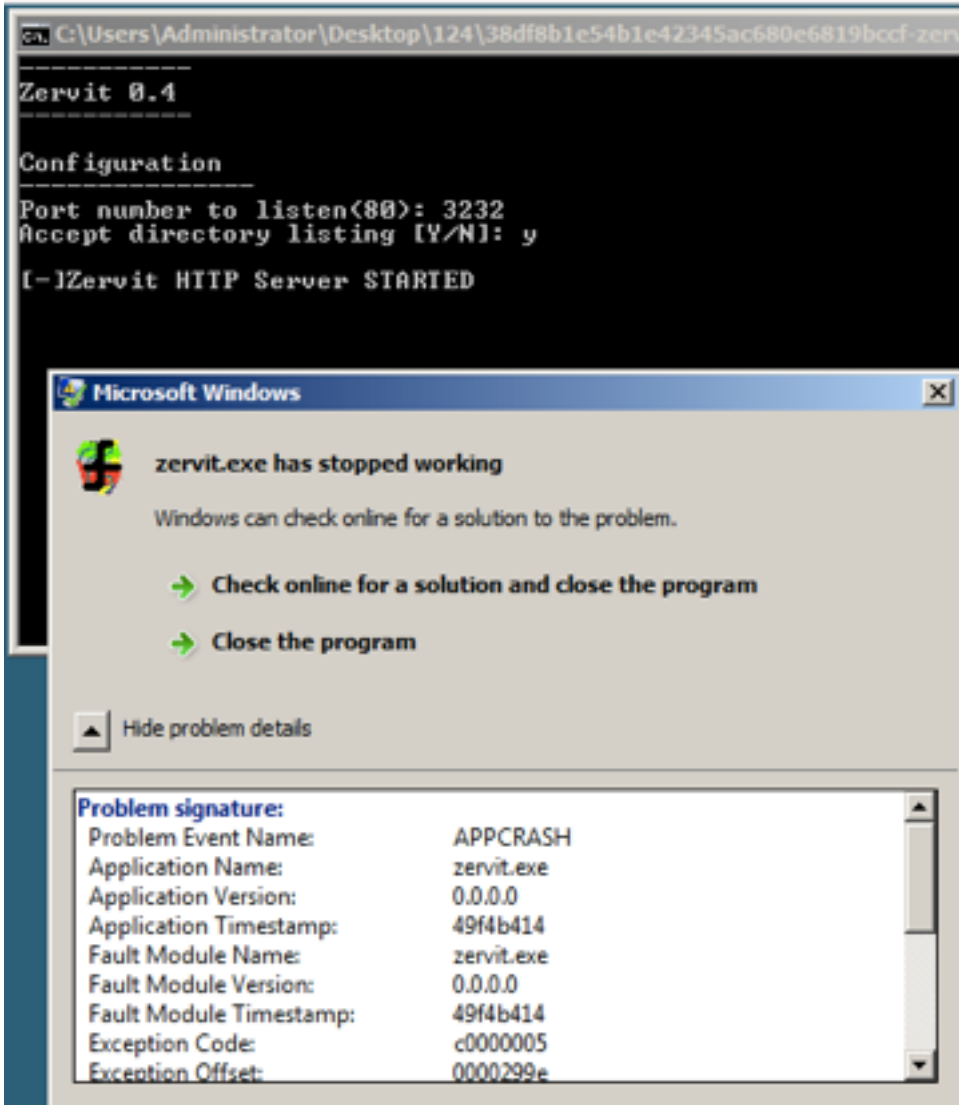
Took 1200 sec.

Scanning Specified Ports

- By default, Nmap scans 1000 "interesting" ports
- You can specify ports with –p switch
- -p 80 will scan one port
- -p 23, 25, 80 will scan three ports
- -p 1-65535 will scan them all (slow)

Nmap Version Scan Crashes Server

- Rarely happens, but is a possibility




Kahoot!