DNS FOR PENETRATION TESTERS

An attacker perspective with a chance of defender discussion

NULL/OWASP/G4H BLR MEET

BHARATH KUMAR

17th June 2017

AGENDA

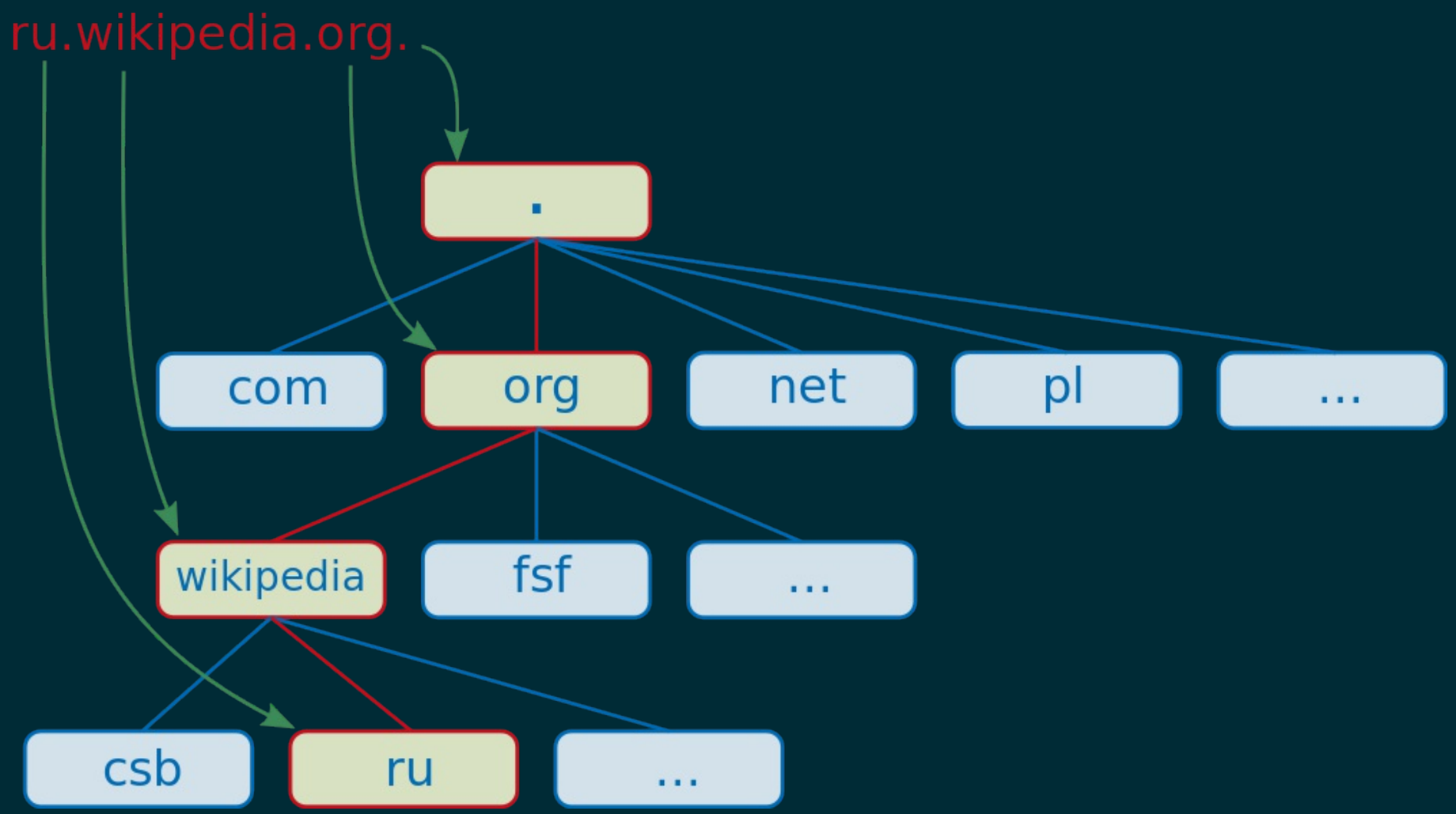
- DNS explained.
- DNS tools.
- DNS attack surface.
- Information gathering through DNS records.
- Mis-configurations in DNS records.
- CAA record & Certificate Transparency.
- Zone transfer attack.
- Zone walking attack.
- Mitigation.

“The Domain Name System, or DNS, is one of the Internet’s fundamental building blocks. It is the ***global***, ***hierarchical***, and ***distributed*** host information database that’s responsible for translating names into addresses and vice versa, routing mail to its proper destination, and many other services.”

bind9.net

DNS IS DISTRIBUTED

DNS IS HIERARCHICAL

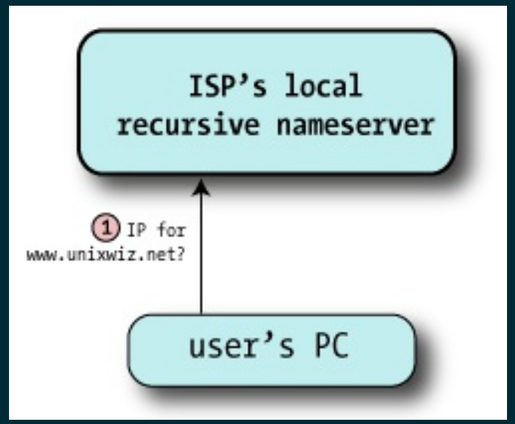

ru.wikipedia.org.
.
com
org
net
pl
...
wikipedia
fsf
...
csb
ru
...

DNS IS GLOBAL

DNS TOOLS

__dig__ if you can, __drill__ if you have to,
__nslookup__ if you must.

DNS RESOLUTION FLOW - STEP I



goo.gl/mRMaZI

RESOLVER

- Resolver is the client part of the DNS client/server system, it asks the questions about hostnames.
- Resolvers are usually very small and dumb, relying on the servers to do the heavy lifting.

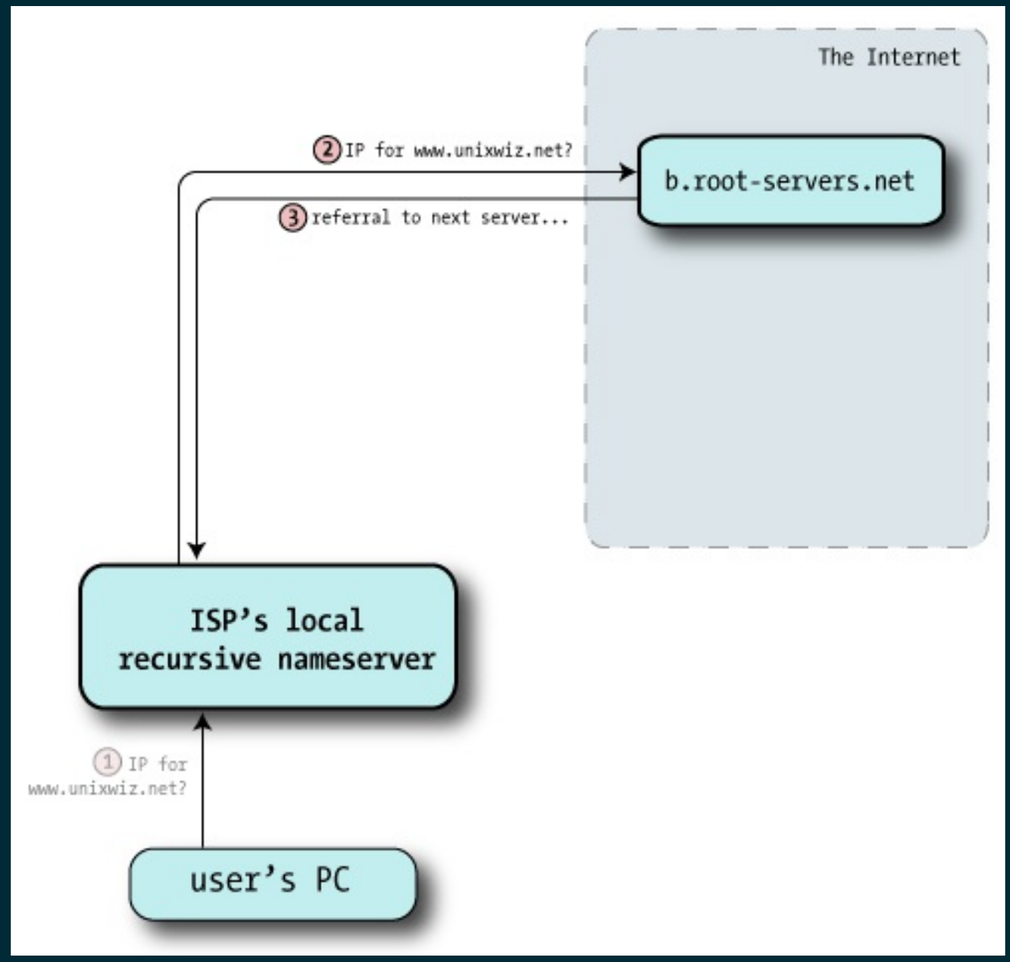
RECURSIVE NAMESERVER

- A nameserver that's willing to go out and find the results for zones it's not authoritative for, as a service to its clients.
- Usually ISP provides raw IP address of recursive DNS servers they maintain, for their customers.
- People unhappy with their ISP's DNS behavior/performance use third-party recursive name servers(open DNS resolvers).

https://www.shodan.io/report/HNgHMj81


8.8.4.4
8.8.8.8

DNS RESOLUTION FLOW - STEP II



goo.gl/mRMaZI

ROOT NAME SERVERS

- Root name servers are at the root of the DNS hierarchy.
- They are authoritative for identifying the name servers responsible for the Top Level Domain (TLD).
- They are a network of hundreds of servers in many countries around the world.
- Shares **13 x 2 IP addresses** (13 IPv4, 13 IPv6) using **Anycast** routing.

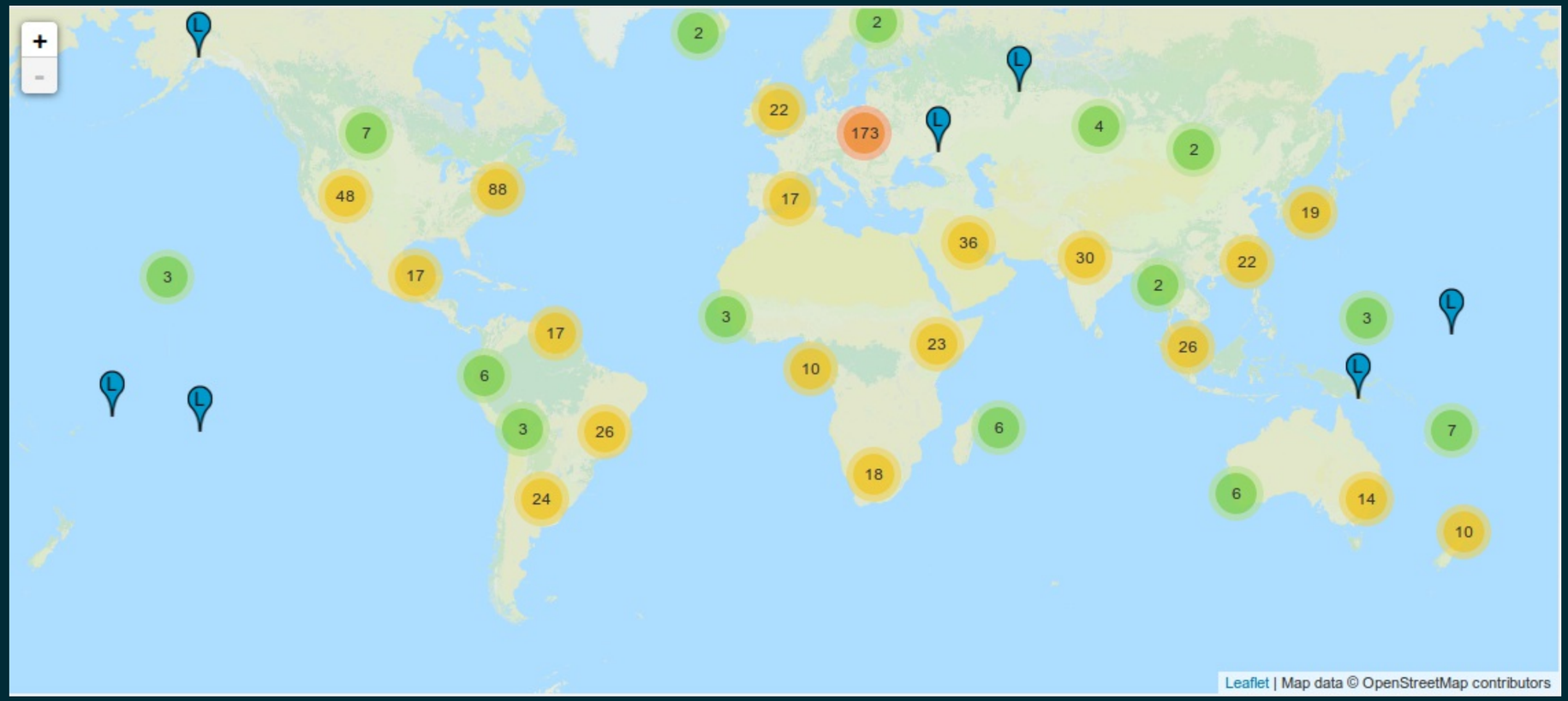
https://www.iana.org/domains/root/servers

List of Root Servers

HOSTNAME	IP ADDRESSES	MANAGER
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	192.228.79.201, 2001:500:200::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

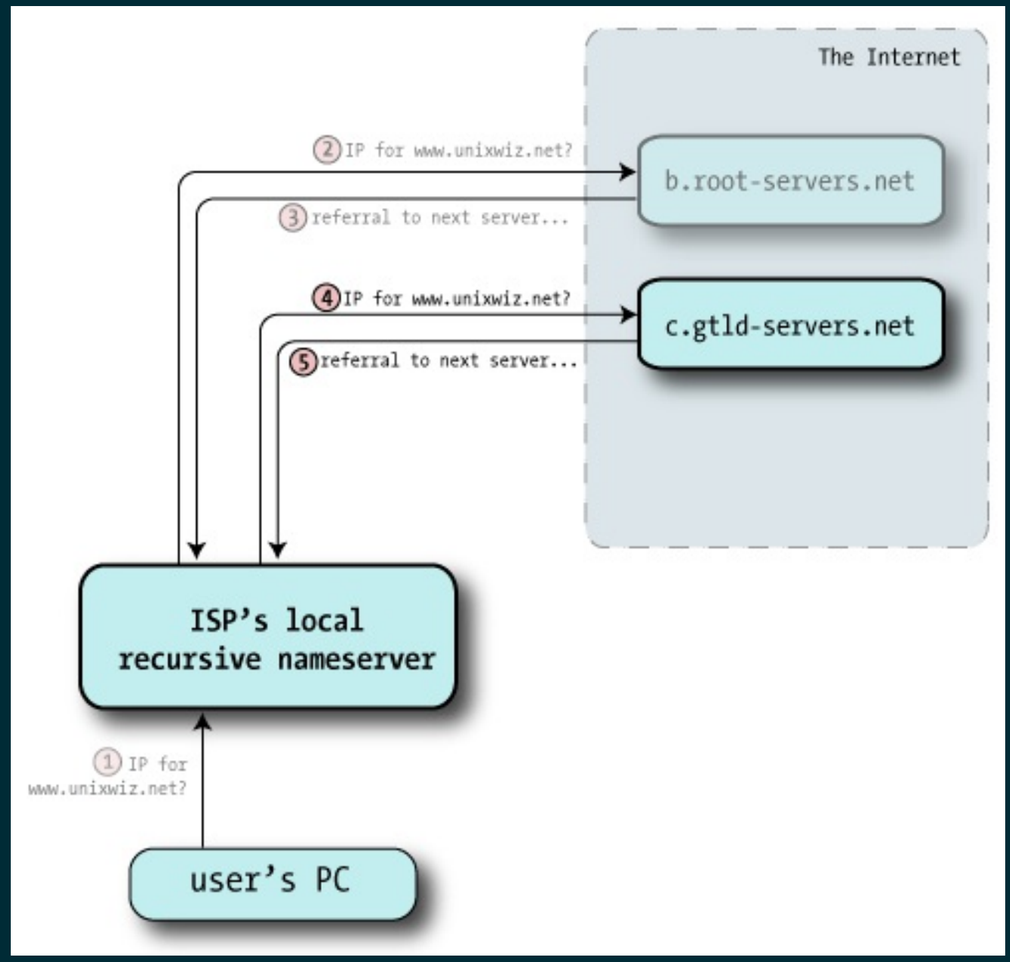
https://www.iana.org/domains/root/servers

ROOT SERVERS MAP



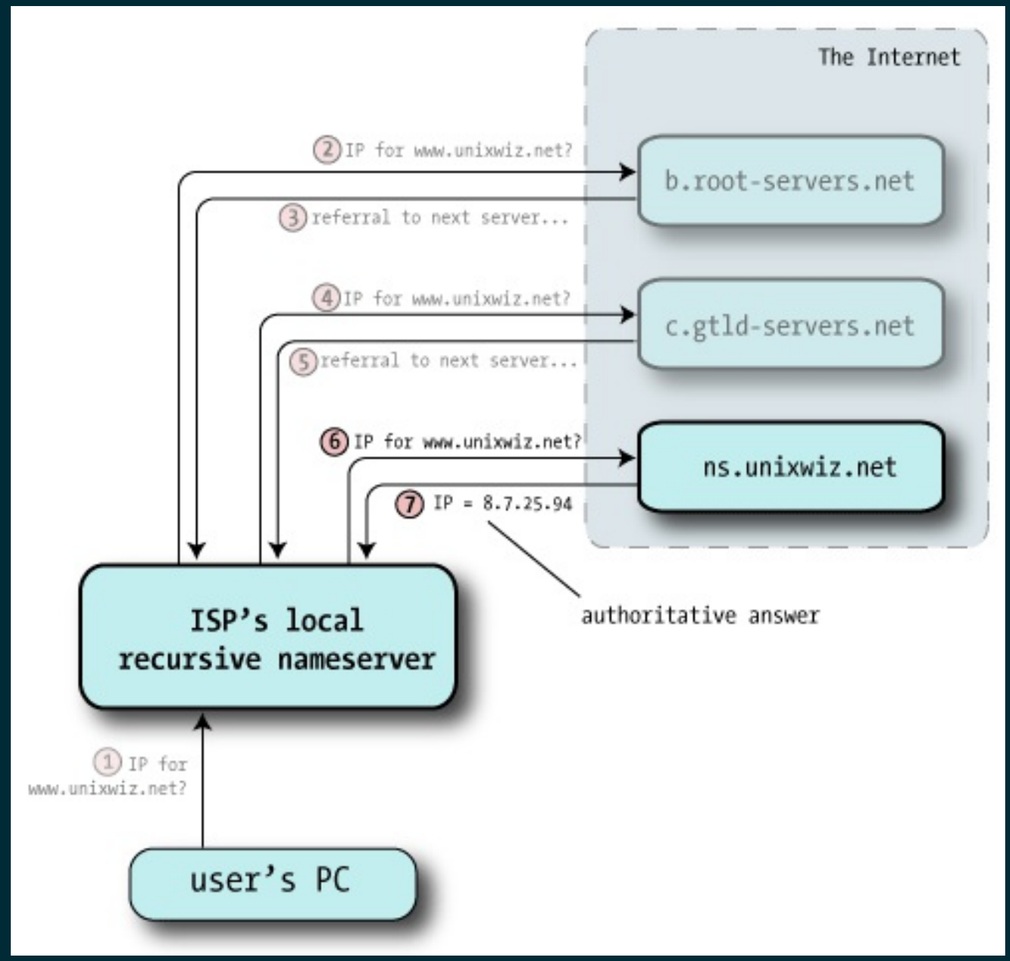
http://www.root-servers.org/

DNS RESOLUTION FLOW - STEP III



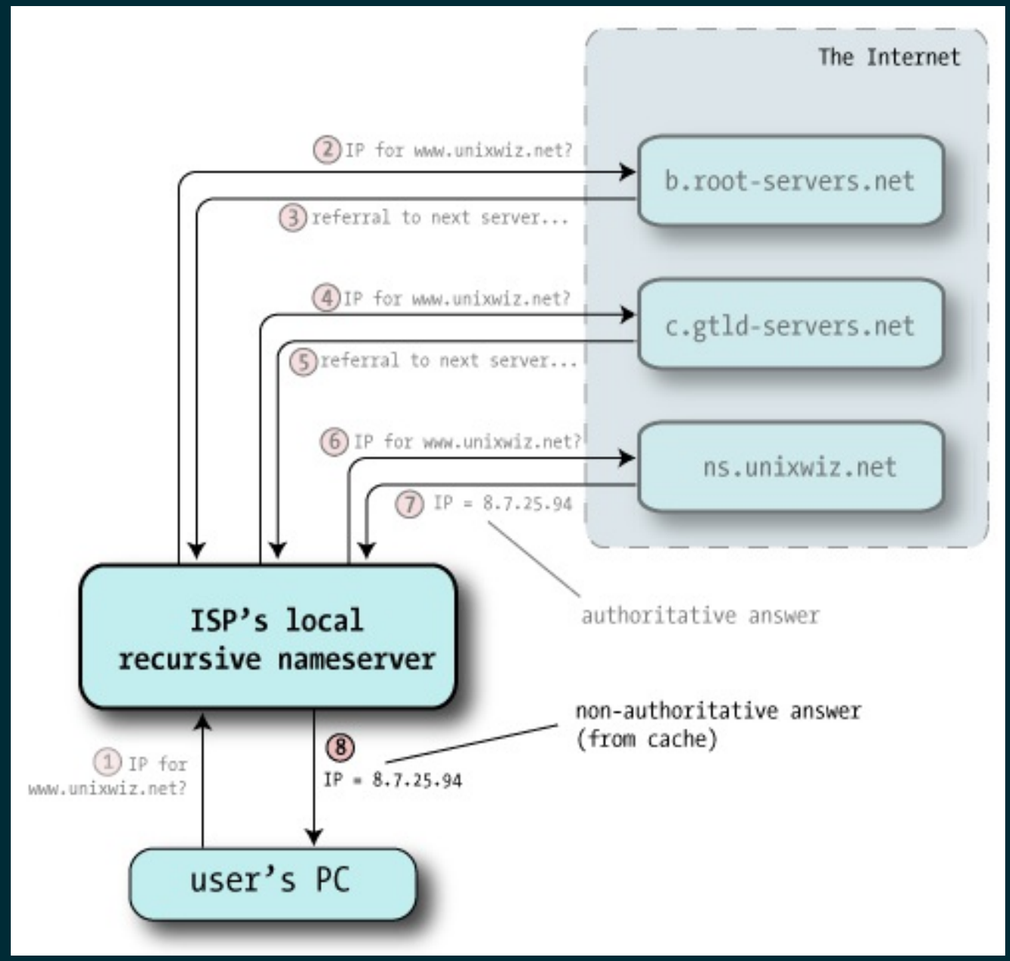
goo.gl/mRMaZI

DNS RESOLUTION FLOW - STEP IV



goo.gl/mRMaZI

DNS RESOLUTION FLOW - STEP V



goo.gl/mRMaZI

DNS RECORDS

Record	Purpose
A	Domain name to an IPv4 adress.
AAAA	Domain name to an IPv6 adress.
PTR	Reverse DNS lookup.(IP address to get hostname.)

DNS RECORDS

Record	Purpose
NS	Nameserver responsible for a given domain.
MX	Mail servers responsible for handling email for the given domain.
SOA	Describes some key data about the zone

DNS RECORDS

Record	Purpose
TXT	A generic Text record that provides descriptive data about domain.
SPF	Identifies which mail servers are permitted to send email on behalf of a given domain
CAA	Specifies which certificate authorities (CAs) are allowed to issue certificates for a domain.

"A" RECORD

- An A record maps a domain name to the IP address (IPv4) of the computer hosting the domain.

```
dig A insecuredns.com
```

```
dig A @8.8.8.8 example.com      # Specify the nameserver with @
```

```
dig +short A iana.org           # Display only the IP addresses
```

"AAAA" RECORD

- AAAA record maps a domain name to the IP address (IPv6) of the computer hosting the domain.

```
dig AAAA insecuredns.com
```

```
dig AAAA @8.8.8.8 example.com    # Specify the nameserver with @
```

```
dig +short AAAA iana.org    # Display only the IP addresses
```

"PTR" RECORD

- Pointer(PTR) records are used to map a network interface (IP) to a host name.
- These are primarily used for reverse DNS.
- Names can reveal information about the host.

```
$ dig +short PTR 4.4.8.8.in-addr.arpa
google-public-dns-b.google.com.
```

```
$ dig +short -x 8.8.8.8
google-public-dns-a.google.com.
```

"NS" RECORD

- An NS record is used to delegate a subdomain to a set of name servers.
- Lists all the name servers responsible for a given domain.

```
dig +short NS insecuredns.com
```

"MX" RECORD

- MX stands for Mail eXchange. MX Records tell email delivery agents where they should deliver your email.
- You can have many MX records for a domain.(For redundancy)
- MX records will reveal any third-party email service being used.

```
dig +short MX insecuredns.com
```

"SOA" RECORD

- Start Of Authority(SOA) record reveals interesting information about the zone.
- Extract primary nameserver:

```
$ dig @8.8.8.8 +short SOA wikipedia.org | cut -d' ' -f1
ns0.wikimedia.org.
```

- Extract email address from zone file.

```
$ dig @8.8.8.8 +short SOA internet.org | cut -d' ' -f2
dns.facebook.com.
```

"TXT" RECORDS

- TXT records hold free form text of any type.
- Special type of TXT records act as SPF, DK, DKIM and DMARC records.
- A lot of third-party service providers use TXT records to verify domain ownership and to ensure email security.

"TXT" RECORDS OSINT ANGLE

- TXT records can reveal third-party services used by the domain.

```
"loaderio=6d3df817ccc37b96c16c78e44b62f75e"
```

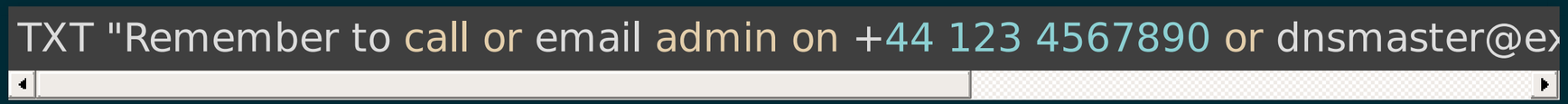
```
"atlassian-domain-verification=+Mx+ ... snipped..."
```

```
"citrix-verification-code=3d0b3642-... snipped..."
```

```
"smartsheet-site-validation.example.com TXT wfJ... snipped..."
```

"TXT" RECORDS OSINT ANGLE

- TXT records are free form so they may hold some interesting info.

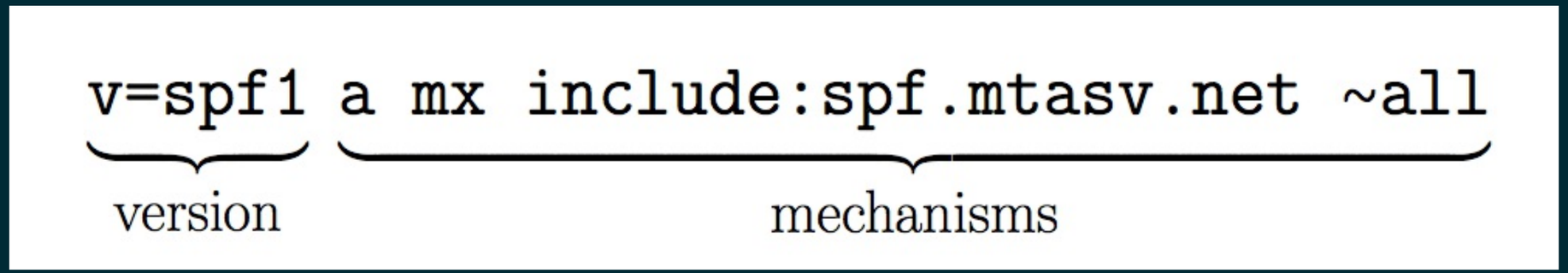


"SPF" RECORDS

- SPF records tells third parties what IP addresses/hostnames are expected to send e-mail of the domain.
- There is a dedicated SPF record type, however, it is deprecated in favor of using a TXT record.

```
300 IN  TXT "v=spf1 a include:spf.mtasv.net ~all"
```

"SPF" RECORD FORMAT



https://postmarkapp.com/blog/explaining-spf

"SPF" RECORD FORMAT

- SPF record can very just point at the domain its self (A, PTR, MX, etc.)

```
v=spf1 a mx include:spf.mtasv.net ~all
          is equivalent to
v=spf1 +a +mx +include:spf.mtasv.net ~all
```

https://postmarkapp.com/blog/explaining-spf

SPF QUALIFIERS

Qualifier	Purpose
+	IP that matches will pass SPF.
-	IP that matches will fail SPF.
~	IP that matches will soft fail SPF.
?	IP that matches will neither pass or fail SPF.

"SPF" SAMPLES

- Allow domain's MXes to send mail for the domain, prohibit all others.

```
"v=spf1 mx -all"
```

- The domain owner thinks that SPF is useless and/or doesn't care.

```
"v=spf1 +all"
```

  - The domain sends no mail at all.

```
"v=spf1 -all"
```

"SPF" BAD PRACTICES

```
v=spf1 all
```

```
v=spf1 +all
```

```
v=spf1 ~ all
```

```
v=spf1include:sendgrid.net~all
```

TL;DR: Use **-all** or **~all** to terminate your SPF record.
(Use DMARC when using SPF softfail)

"SPF" OSINT ANGLE

- SPF records reveal third-party mail providers that the domain may rely on.

```
"v=spf1" "include:_spf.google.com" "include:mail.zendesk.com" "-all"
```

- SPF sometimes reveals IP addresses (and net blocks) of the organization that you may not have been aware of.

```
"v=spf1 ip4:208.118.237.0/24 ip4:208.118.227.0/25 ip4:64.125.235.5 ip4:64.
```

goo.gl/vQPCtB

CAA RECORD

- A Certification Authority Authorization (CAA) record is used to specify which certificate authorities (CAs) are allowed to issue certificates for a domain.
- The idea is to allow domain owners to declare which certificate authorities are allowed to issue a certificate for a domain.

```
example.com.  CAA 0 issue "letsencrypt.org"
```

CAA RECORDS

- **issue** tag identifies CA that is authroized to issue certificate
- **issuewild** tag identifies CA that is authorized to issue wildcard certificates.
- **iodef** contains an email address to notify in case a violation is detected.

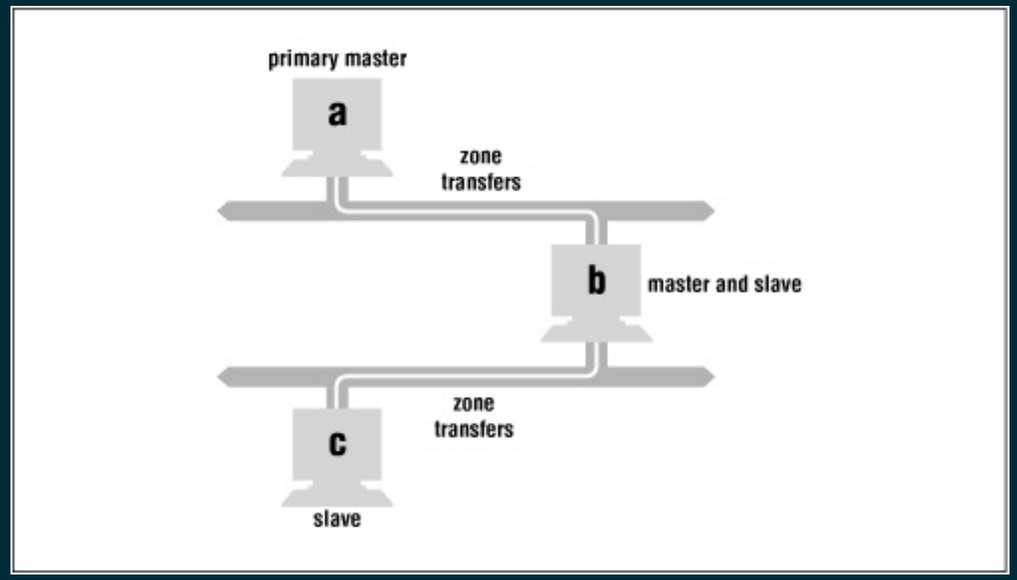
```
example.com.    1200    IN  CAA 0 issue "comodoca.com"
example.com.    1200    IN  CAA 0 issuewild "comodoca.com"
example.com.    1200    IN  CAA 0 iodef "mailto:sslabuse@example.com"
```

CERTIFICATE TRANSPARENCY(CT)

- Certificate Transparency is a recent IETF standard, under which CAs will have to publish all SSL/TLS certificates they issue in a public log.
- Using CT and CAA records, it's easy to identify rogue/fraudelent SSL/TLS certificates in the wild.

ZONE TRANSFER(ATTACK)

- zone transfer is a type of DNS transaction where a DNS server passes a copy of part of it's database(zone file) to another DNS server.
- DNS zone transfer is always initiated by client/slave by inducing **DNS query type AXFR**.



ZONE TRANSFER(ATTACK)

```
$ dig AXFR @ns1.iitk.ac.in. iitk.ac.in
iitk.ac.in.     43200   IN  SOA ns1.iitk.ac.in. root.ns1.iitk.
iitk.ac.in.     43200   IN  NS  ns2.iitk.ac.in.
iitk.ac.in.     43200   IN  NS  proxy.iitk.ac.in.
home.iitk.ac.in.    43200   IN  A   202.3.77.174
m3cloud.iitk.ac.in. 43200   IN  A   103.246.106.161
mail.iitk.ac.in.    43200   IN  A   202.3.77.162

[... snipped ...]

mail4.iitk.ac.in.   43200   IN  A   202.3.77.189
webmail.iitk.ac.in. 43200   IN  A   202.3.77.185
www.webmap.iitk.ac.in.  43200   IN  A   202.3.77.74
wiki.iitk.ac.in.    43200   IN  A   103.246.106.116
www.iitk.ac.in.     43200   IN  A   202.3.77.184
```

DNSSEC IN 2 MINS

- DNSSEC is normal DNS, but with cryptographic signatures. It prevents DNS Spoofing.
- DNSSEC provides a layer of security by adding cryptographic signatures to existing DNS records.
- These signatures are stored alongside common record types like A, AAAA, MX etc.
- By checking associated signature, you can verify that a requested DNS records comes from authoritative nameserver and not spoofed.

AUTHENTICATED DENIAL OF EXISTENCE IN THE DNS

- DNSSEC must assert the non-existence of records in a zone to prevent attackers spoofing NXDOMAIN responses in an attempt at denial-of-service.
- Your zone is sorted alphabetically, and the NextSECure(NSEC) records point to the record after the one you looked up.
- Using NSEC is relatively simple, but it has a nasty side-effect: it allows anyone to list the zone content by following the linked list of NSEC records.
- Detailed explaination - Take your DNSSEC with a grain of salt

ZONE WALKING - NSEC

- The ldns library contains an tool called ldns-walk that can be used to list all records inside a DNSSEC signed zone that uses NSEC.

```
$ ldns-walk iana.org
iana.org.    iana.org. A NS SOA MX TXT AAAA RRSIG NSEC DNSKEY
api.iana.org. CNAME RRSIG NSEC
app.iana.org. CNAME RRSIG NSEC
autodiscover.iana.org. CNAME RRSIG NSEC
beta.iana.org. CNAME RRSIG NSEC
blackhole-1.iana.org. A AAAA RRSIG NSEC
blackhole-2.iana.org. A AAAA RRSIG NSEC
blackhole-3.iana.org. AAAA RRSIG NSEC
blackhole-4.iana.org. AAAA RRSIG NSEC
data.iana.org. CNAME RRSIG NSEC
datatracker.iana.org. CNAME RRSIG NSEC
dev.iana.org. CNAME RRSIG NSEC
ftp.iana.org. CNAME RRSIG NSEC
svn.int.iana.org. CNAME RRSIG NSEC
itar.iana.org. A AAAA RRSIG NSEC
```

ZONE WALKING - NSEC3

- The NSEC3 record option in DNSSEC solves this by creating the linked list using hashed domain-names, instead of clear-text domain names.
- It is possible to collect all the hashes and crack them offline using rainbow tables.
- Tools like nsec3map will collect hashes and crack them offline.

```
i8enajodqvfjd9t90he4svha3kgntc12.icann.org.    3600    IN    NSEC3
djg1irkar2s8d0cka16kio1ribpcmuqp.icann.org.    3600    IN    NSEC3
vrt34mkpiesf3fc6kdoovv7irv67odem.icann.org.    3600    IN    NSEC3
3eu2lrfspij2g37gvr2b75sop5rfev92.icann.org.    3600    IN    NSEC3
qn21dpjn6etm2udq8k4t8v828ou4ege1.icann.org.    3600    IN    NSEC3
gp8mhqp858u55rd62v7inl54m5lmf046.icann.org.    3600    IN    NSEC3
```

PASSIVE RECON USING PUBLIC DATASETS

- **scans.io** and **Project Sonar** gather Internet wide scan data and make it available to researchers and the security community.
- This data includes port scans and a dump of all the DNS records that they can find.
- Find your needle in the haystack.

REFERENCES

- http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html
- https://postmarkapp.com/blog/explaining-spf
- https://www.cloudflare.com/dns/dnssec/how-dnssec-works/
- https://strotmann.de/roller/dnsworkshop/entry/take_your_dns

BHARATH KUMAR

- Security research @Appsecco
- Offensive Security Certified Professional(OSCP)
- http://twitter.com/yamakira_
- http://github.com/yamakira
- http://disruptivelabs.in