

ESOTERIC SUB-DOMAIN ENUMERATION TECHNIQUES



BHARATH KUMAR

BUGCROWD LEVELUP | JULY 15TH 2017

ABOUT ME

- Bharath Kumar
- Security Engineer @Appsecco
- Offensive Security Certified Professional(OSCP)
- I enjoy good books, coffee, camping and stargazing!

DEMO ENVIRONMENT

- Feel free to run the DNS & DNSSEC attacks from the talk against the following nameserver & domain:

Nameserver: **ns1.insecuredns.com**

Domain: **insecuredns.com**

WHAT IS THIS TALK ABOUT?

- Sub-domain enumeration
- Esoteric sub-domain enumeration
- We'll discuss techniques, tools and mitigation


WHAT IS SUB-DOMAIN ENUMERATION?

Sub-domain enumeration is the process of finding sub-domains for one or more domain(s).

WHY SUB-DOMAIN ENUMERATION?


Finding applications running on hidden, forgotten sub-domains may lead to uncovering critical vulnerabilities

XSS ON SALESFORCE SUB-DOMAIN

 admin.salesforce.com subdomain was actually used by Salesforce for blogging purposes. It was susceptible to a reflected Cross-site Scripting (XSS) vulnerability, whereby a specific function in the deployed application failed to

YAHOO! VOICES HACK

Yahoo! Voice a.k.a Associated Content. *"The affected website was only named as a sub-domain of yahoo.com. However, digging through and searching for the hostname, the attacker forgot to remove the hostname "dbb1.ac.bf1.yahoo.com" (credit to Mubix for the hostname*




SYSTEMA SOFTWARE DATA BREACH

A treasure trove of personal information on around 1.5 million US insurance claimants has been discovered in clear text on a publicly available Amazon Web Services subdomain.



XSS ON EBAY SUB-DOMAIN

discovered the bug and disclosed it to eBay, Aditya Sood. The vulnerability existed on an eBay subdomain, `svcs.ebay.com`, and Sood said it specifically was in the SMS gateway on the page.



COMMON SUB-DOMAIN ENUMERATION TECHNIQUES

1. Google dorking
2. Using specialized search engines
3. Dictionary based enumeration
4. Sub-domain bruteforce
5. ASN discovery

WHAT DOES ESOTERIC MEAN?

esoteric

/,ɛsə'terɪk,,i:sə'terɪk/ 🔊

adjective

intended for or likely to be understood by only a small number of people with a specialized knowledge or interest.

"esoteric philosophical debates"

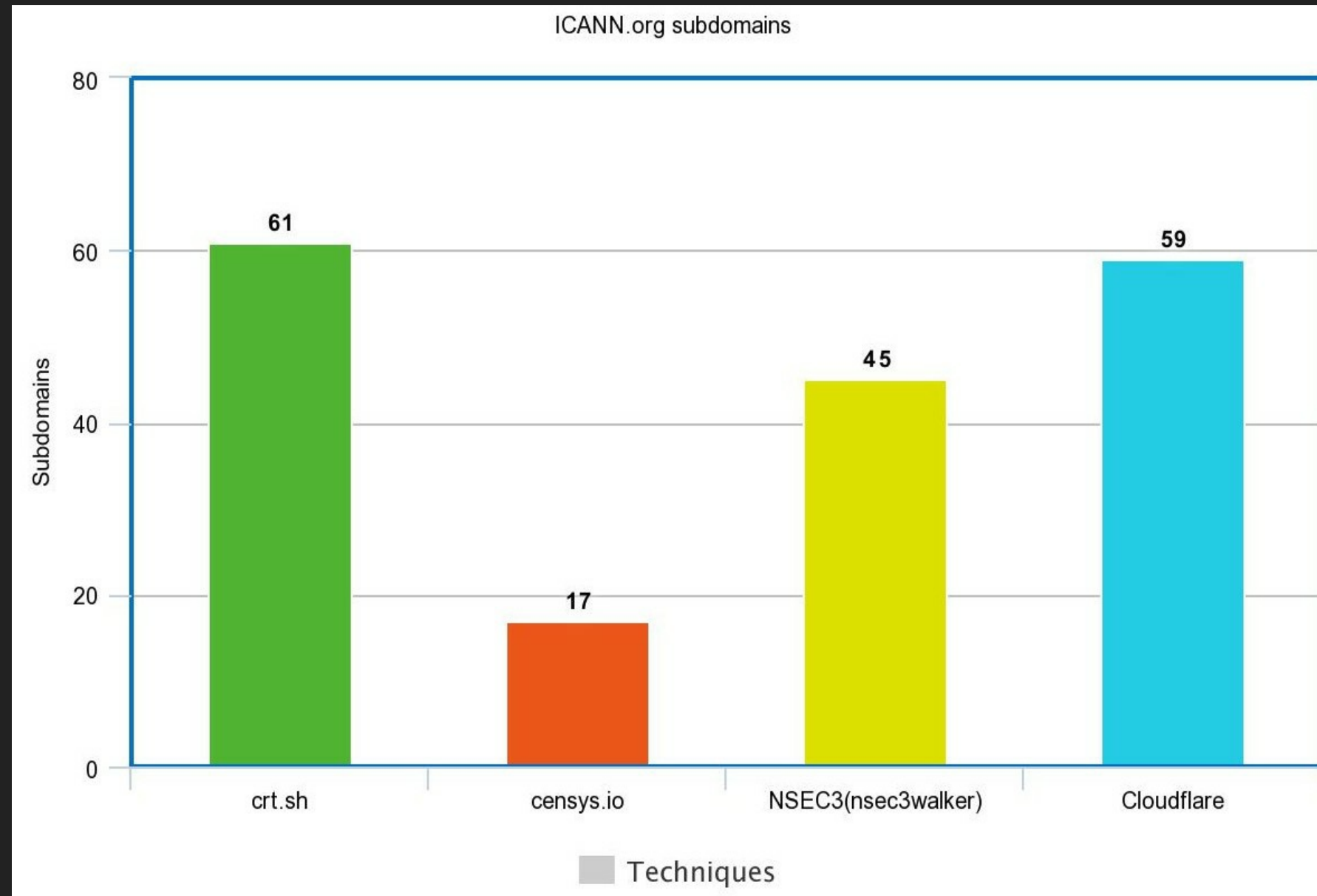
synonyms: [abstruse](#), [obscure](#), [arcane](#), [recherché](#), [rarefied](#), [recondite](#), [abstract](#), [difficult](#), [hard](#), [puzzling](#), [perplexing](#), [enigmatic](#), [inscrutable](#), [cryptic](#), [Delphic](#); [More](#)

TECHNIQUES WE'LL LOOK INTO

1. Certificate Transparency
2. DNSSEC zone walking
3. DNS zone transfer
4. Passive recon using public datasets

ICANN.ORG SUBDOMAINS

Number of unique subdomains each technique found independently against icann.org



CERTIFICATE TRANSPARENCY(CT)

- Under CT, a Certificate Authority(CA) will have to publish all SSL/TLS certificates they issue in a public log
- Anyone can look through the CT logs and find certificates issued for a domain


CT - SIDE EFFECT

- CT logs by design contain all the certificates issued by a participating CA for any given domain
- By looking through the logs, **an attacker can gather a lot of information** about an organization's infrastructure i.e. internal domains, email addresses in a **completely passive manner**

SEARCHING THROUGH CT LOGS

- There are various search engines that collect the CT logs and let's anyone search through them
 1. <https://crt.sh/>
 2. <https://censys.io/>
 3. <https://google.com/transparencyreport/https/ct/>

Searching SSL/TLS certificates issued for a domain

<div><div>crt.sh</div><div>Identity Search</div><div></div><div>Group by Issuer</div></div>				
Criteria		Identity LIKE %		
crt.sh ID	Logged At ↑	Not Before	Identity	Issuer Name
	2017-06-19	2017-06-19	roubir.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2017-06-19	2017-06-19	www.roub.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2017-06-19	2017-06-19	levelup.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2017-06-15	2017-06-13	*.com	C=US, O=Amazon, OU=Server CA 1B, CN=Amazon
	2017-05-27	2017-05-26	support.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
	2017-05-26	2017-05-24	content1.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
	2017-05-26	2017-05-24	content1.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
	2017-05-26	2017-05-24	content2.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
	2017-05-26	2017-05-24	content2.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
	2017-05-26	2017-05-24	content.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
	2017-05-26	2017-05-24	content.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
	2017-05-26	2017-05-24	drupal.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
	2017-05-26	2017-05-24	drupal.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
	2017-05-26	2017-05-24	drupal.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
	2017-05-26	2017-05-24	edit.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
	2017-05-26	2017-05-24	edit.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
	2017-05-26	2017-05-24	qullqa.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
	2017-05-26	2017-05-24	qullqa.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
	2017-05-26	2017-05-24	*.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
	2017-05-26	2017-05-24	webteam.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
	2017-05-26	2017-05-24	www.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
	2017-05-26	2017-05-24	www.com	C=US, O=DigiCert Inc, CN=DigiCert SHA2 Secure Server CA
	2017-05-20	2017-05-20	levelup.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Output of a script that searches through CT Logs for a given domain and extracts sub-domains & emails

```
*.com
marketplace.com
lon.com
citi.com
dropbox.com
debdmz1.com
klk.com
ny.com
docserver.com
icloud.com
staging-demopartner.com
india.com
london.com
jabber.com
boatest.com
filer.com
msu.com
atl.com
blm.com
cedar-uat.com
.com
myssi.com
cs.com
portal-waf.com
cac.com
mx43.us
staging-cedar-sp.com
*.expert.com
esp.com
indy.com
ibm-secure.com
cedar.sp.com
finished in 2.361

8600.com
systems.com
root@fmtstdmngins02.com
root@elkdmzproxy01.com
root@chidmzhosting03.com
ylli.com
www.com
jgumbley.com
d-cent.com
hcah_dev.com
cford.com
mingle.saas.com
delta_dev.com
www-devs.com
jim.com
csun.com
aleite.com
jedwards.com
recruiting-dev.com
bjanakir.com
scxu.com
bhkwan.com
```

DEMO TIME

ENUMERATING SUB-DOMAINS USING CT LOGS

CT LOGS - MITIGATION

- Not have SSL/TLS support. This approach is definitely not recommended
- Deploy your own Public Key Infrastructure(PKI)
- Opt out of CT logs but you'll miss out on all the security benefits that CT provides
- Name redaction in CT logs let's you hide your sub-domain information in a CT log

DNSSEC

- 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

DNSSEC - NEW RECORDS

Record	Purpose
RRSIG	Contains a cryptographic signature.
NSEC and NSEC3	For explicit denial-of-existence of a DNS record
DNSKEY	Contains a public signing key
DS	Contains the hash of a DNSKEY record

DNSSEC - AUTHENTICATED DENIAL OF EXISTENCE(RFC 7129)

In DNS, when client queries for a non-existent domain, the server must deny the existence of that domain. It is harder to do that in DNSSEC due to cryptographic signing.

PROBLEMS WITH AUTHENTICATED DENIAL OF EXISTENCE(DNSSEC)

1. *NXDOMAIN* responses are generic, attackers can spoof the responses
2. Signing the responses on the fly would mean a performance and security problem
3. Pre-signing every possible *NXDOMAIN* record is not possible as there will be infinite possibilities

NSEC

- Zone entries are sorted alphabetically, and the NextSECure(NSEC) records point to the record after the one you looked up
- Basically, NSEC record says, “there are no subdomains between sub-domain X and sub-domain Y.”

```
$ dig +dnssec @ns1.insecuredns.com firewallll.insecuredns.com
... snipped ...
firewall.insecuredns.com. 604800 IN NSEC mail.insecuredns.com. A RRSIG
... snipped ...
```

ZONE WALKING NSEC - LDNS

- The `ldns-walk`(part of `ldnsutils`) can be used to zone walk DNSSEC signed zone that uses NSEC.

```
# zone walking with ldnsutils
$ 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
data.iana.org. CNAME RRSIG NSEC
dev.iana.org. CNAME RRSIG NSEC
ftp.iana.org. CNAME RRSIG NSEC
^C
```

INSTALLING LDNSUTILS

```
# On Debian/Ubuntu  
$ sudo apt-get install ldnutils
```

```
# On Redhat/CentOS  
$ sudo yum install ldns  
# You may need to do  
$ sudo yum install -y epel-release
```

ZONE WALKING NSEC - DIG

- You can list all the sub-domains by following the linked list of NSEC records of existing domains.

```
$ dig +short NSEC api.nasa.gov  
apm.nasa.gov. CNAME RRSIG NSEC
```

```
$ dig +short NSEC apm.nasa.gov  
apmcpr.nasa.gov. A RRSIG NSEC
```

EXTRACTING THE SUB-DOMAIN FROM NSEC

- You can extract the specific sub-domain part using `awk` utility.

```
$ dig +short NSEC api.nasa.gov | awk '{print $1;}'  
apm.nasa.gov.
```

DEMO TIME

ZONE WALKING USING NSEC RECORDS

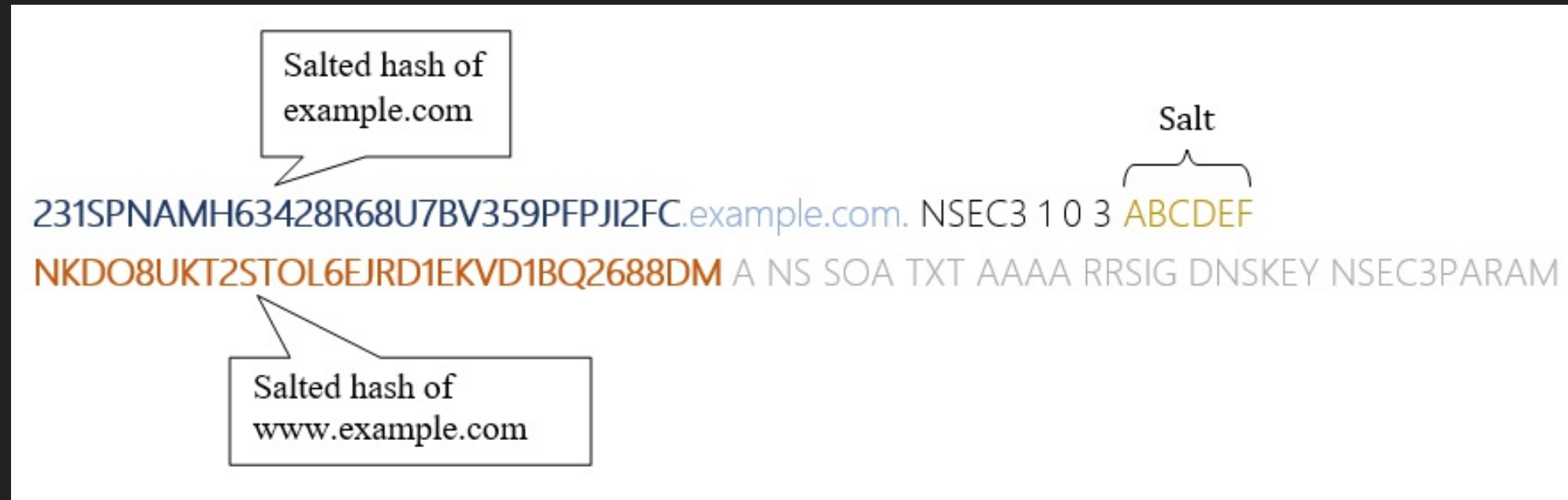
NSEC3

- The NSEC3 record is like an NSEC record, but, NSEC3 provides a signed gap of hashes of domain names.
- Returning hashes was intended to prevent zone enumeration(or make it expensive).

```
231SPNAMH63428R68U7BV359PFPJI2FC.example.com. NSEC3 1 0 3 ABCD  
NKDO8UKT2STOL6EJRD1EKVD1BQ2688DM A NS SOA TXT AAAA RRSIG DN
```

```
NKDO8UKT2STOL6EJRD1EKVD1BQ2688DM.example.com. NSEC3 1 0 3 AB  
231SPNAMH63428R68U7BV359PFPJI2FC A TXT AAAA RRSIG
```


NSEC3 - LINKED LIST OF HASHES



GENERATING NSEC3 HASH FOR A DOMAIN NAME

- `ldns-nsec3-hash`(part of `ldnsutils`) generates NSEC3 hash of domain name for a given salt value and number of iterations
- Number of iterations & salt value is available as part of NSEC3 record.

```
$ ldns-nsec3-hash -t 3 -s ABCDEF example.com  
231spnamh63428r68u7bv359pfpji2fc.
```

```
$ ldns-nsec3-hash -t 3 -s ABCDEF www.example.com  
nkdo8ukt2stol6ejrd1ekvd1bq2688dm.
```

ZONE WALKING NSEC3

- An attacker can collect all the sub-domain hashes and crack the hashes offline
- Tools like *nsec3walker*, *nsec3map* help us automate collecting NSEC3 hashes and cracking the hashes

ZONE WALKING NSEC3

Zone walking NSEC3 protected zone using
nsec3walker:

```
# Collect NSEC3 hashes of a domain  
$ ./collect insecuredns.com > insecuredns.com.collect
```

```
# Undo the hashing, expose the sub-domain information.  
$ ./unhash < insecuredns.com.collect > insecuredns.com.unhash
```

ZONE WALKING NSEC3

```
# Checking the number of successfully cracked sub-domain hashes
```

```
$ cat icann.org.unhash | grep "icann" | wc -l
```

```
45
```

```
# Listing only the sub-domain part from the unhashed data
```

```
$ cat icann.org.unhash | grep "icann" | awk '{print $2;}'
```

```
del.icann.org.
```

```
access.icann.org.
```

```
charts.icann.org.
```

```
communications.icann.org.
```

```
fellowship.icann.org.
```

```
files.icann.org.
```

```
forms.icann.org.
```

```
mail.icann.org.
```

```
maintenance.icann.org.
```

```
new.icann.org.
```

```
public.icann.org.
```

```
research.icann.org.
```

```
rs.icann.org.
```

INSTALLING NSEC3WALKER

- Installation instructions are available at <https://dnscurve.org/nsec3walker.html>
- I used following commands to install nsec3walker on Ubuntu 16.04.
 - build-essential package is a prerequisite.

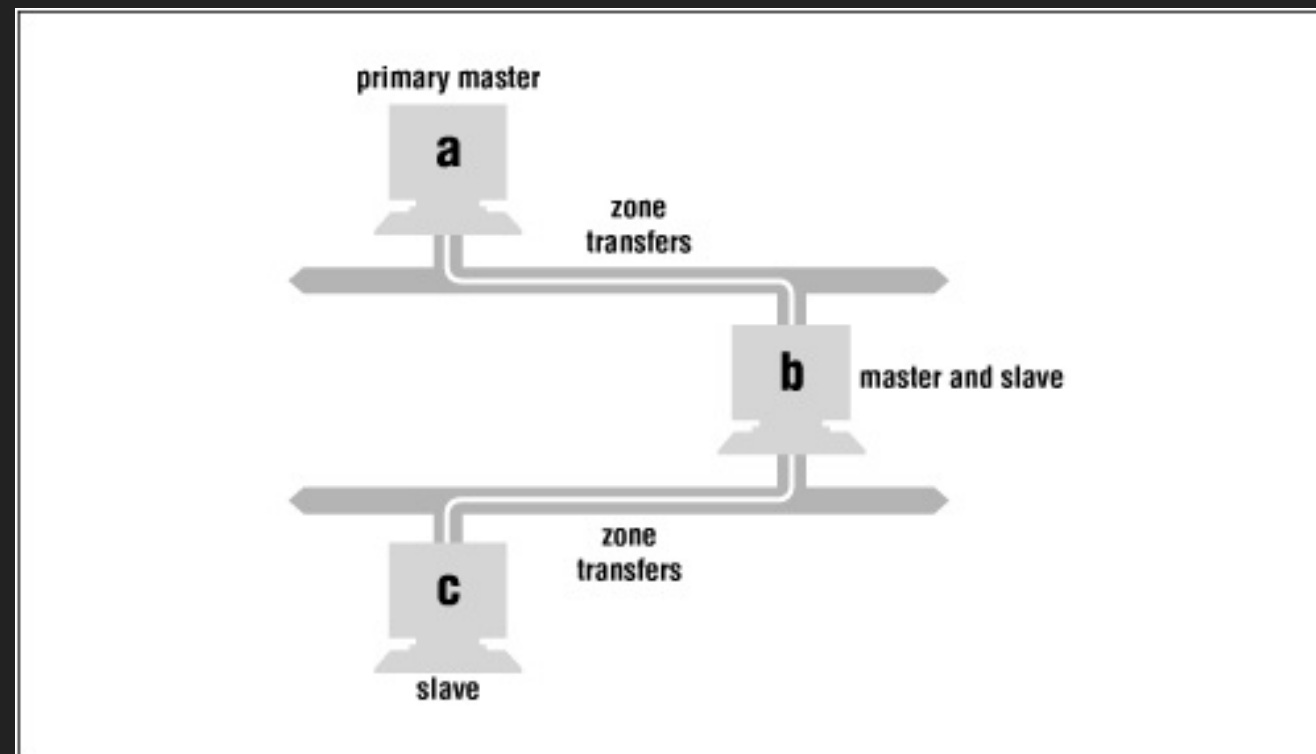
```
# Installing nsec3walker
$ wget https://dnscurve.org/nsec3walker-20101223.tar.gz
$ tar -xzf nsec3walker-20101223.tar.gz
$ cd nsec3walker-20101223
$ make
```

DEMO TIME

ZONE WALKING NSEC3 PROTECTED ZONE

ZONE TRANSFER

- Zone transfer is a type of DNS transaction where a DNS server passes a copy of part of its zone file to another DNS server.



ZONE TRANSFER(ATTACK)

- If zone transfers are not securely configured, anyone can initiate a zone transfer against a nameserver and get a copy of the zone file.
- By design, zone file contains a lot of information about the zone and the hosts that reside in the zone.

ZONE TRANSFER USING *DIG*

```
$ 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
```

DEMO TIME

ZONE TRANSFER USING *DIG*

IS ZONE TRANSFER RELEVANT ANYMORE?

- Global zone transfers are hard to find on public DNS servers.
- It's common to find DNS servers with liberal zone transfer permissions in internal networks.
- Even the top level nameservers were accidentally configured to allow global DNS zone transfers.
 1. North Korea DNS leak
 2. Russian DNS leak

ZONE TRANSFER - MITIGATION

- You can allow only specific IP addresses to initiate zone transfer against a nameserver
- The allow-transfer feature(in Bind) can be used to configure permissions

```
# /etc/bind/named.conf.options has global bind settings.  
$ cat named.conf.options | grep "allow-transfer"  
allow-transfer { none; };
```

```
# /etc/bind/named.conf.local has config for individual zones  
zone "insecuredns.com" {  
    type master;  
    file "/etc/bind/zones/db.insecuredns.com.signed";  
    allow-transfer { 192.168.56.1; };  
};
```

EVADING IP BASED MITIGATION

- IP based restrictions are susceptible to IP address spoofing
- In an internal pentest, you can pretend to be the secondary nameserver, initiate a zone transfer and sniff the zone data

ZONE TRANSFER - MITIGATION

- An added layer of security is to deploy DNS Transaction Signatures(TSIG) between the DNS nameservers
- TSIG uses shared secret keys and one-way hashing to provide a cryptographically secure means of authenticating each endpoint of a connection as being allowed to make or respond to a DNS update

WHAT IS PASSIVE RECONNAISSANCE?

- In passive reconnaissance, an attacker gathers information without generating any traffic directly between him and the infrastructure managed by the target organization
- The objective is to be stealthy and leave low or no footprint

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.

PASSIVE RECON USING PUBLIC DATASETS

- Rapid7 publishes its Forward DNS study/dataset on scans.io project(it's a massive dataset, 20+ GB)
- This dataset aims to discover all domains found on the Internet
- The data format is a gzip-compressed JSON file so we can use jq utility to extract sub-domains of a specific domain:

```
zcat 20170204-fdns.json.gz | \
jq -r 'if (.name | test("\\.example\\.com$")) \
then .name else empty end'
```

Subdomain enumeration cheat sheet

Certificate Transparency logs - search engines

<https://crt.sh/>

<https://censys.io/>

<https://google.com/transparencyreport/https/ct/>

Extracting sub-domains from Rapid7 FDNS dataset

```
$ zcat <dataset_name> | jq -r 'if (.name | test("\\.example\\.com$")) then .name else empty end'
```

```
$ zcat 20170204-fdns.json.gz | jq -r 'if (.name | test("\\.example\\.com$")) then .name else empty end'
```

Rapid7 - Forward DNS dataset
https://scans.io/study/sonar.fdns_v2

Zone walking - NSEC

```
$ ldns-walk @<nameserver> <domain>
```

```
$ ldns-walk @ns1.insecuredns.com  
insecuredns.com
```

Installing ldns utilities

```
$ sudo apt-get install ldnsutils #
```

On Ubuntu/Debian

```
$ yum install ldns # On
```

Redhat/CentOS

Zone transfer

```
$ dig AXFR @<nameserver> <domain>
```

```
$ dig AXFR @ns1.insecuredns.com  
insecuredns.com
```

Zone walking - NSEC3 - nsec3walker

```
$ ./collect insecuredns.com >  
insecuredns.com.collect
```

```
$ ./unhash <  
insecuredns.com.collect >  
insecuredns.com.unhash
```

Installing nsec3walker on Ubuntu 16.04:

```
$ wget
```

<https://dnscurve.org/nsec3walker-20101223.tar.gz>

```
$ tar -xzf
```

```
nsec3walker-20101223.tar.gz
```

```
$ cd nsec3walker-20101223
```

```
$ make
```



Bharath
@yamakira

BONUS ROUND

MAKING CLOUDFLARE DO DNS ENUMERATION FOR YOU

- When you try to "Add site" to cloudflare account, cloudflare does some DNS enumeration and finds sub-domains that belong to the domain you entered

DNS ENUMERATION THROUGH CLOUDFLARE

1. Login into cloudflare
<https://www.cloudflare.com/login>
2. "Add site" to your account
<https://www.cloudflare.com/a/add-site>
3. Provide the target domain as a site you want to add
4. Wait for cloudflare to dig through DNS data and display the results

DNS ENUMERATION THROUGH CLOUDFLARE

https://www.cloudflare.com/a/setup/icann.org/step/2

n.org		
	CNAME	info is an alias of icann.mktoweb.com
	CNAME	internal is an alias of internal.vip.icann.org
	CNAME	jira is an alias of jira.vip.icann.org
	CNAME	labs is an alias of archive.vip.icann.org
	CNAME	learn is an alias of icann.usefedora.com
	CNAME	maintenance is an alias of maintenance.vip.icann.org
	CNAME	me is an alias of redirects.icann.org
	CNAME	meet is an alias of meet.vip.icann.org
	CNAME	members is an alias of archive.vip.icann.org

DNS ENUMERATION THROUGH CLOUDFLARE

- [Matthew Bryant](#) wrote a neat little script to automate this process

```
[dante@machina: ~/code_repos/cloudflare_enum]
->$ python cloudflare_enum.py [redacted]@gmail.com agoda.com
Provide your cloudflare password:

Cloudflare DNS Enumeration Tool v1.3
Created by mandatory
Modified by yamakira

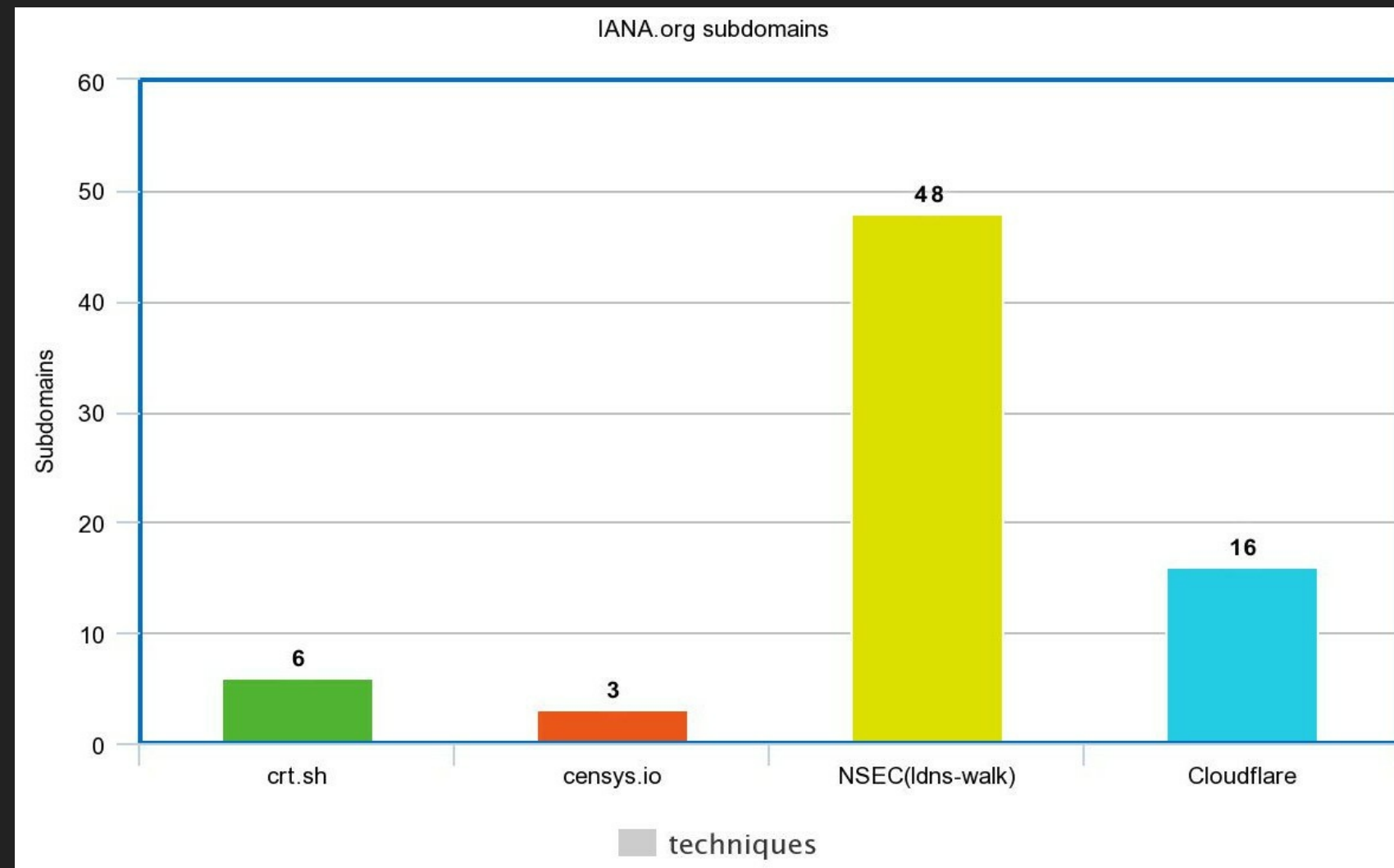
[ STATUS ] Spreadsheet created at /home/dante/code_repos/cloudflare_enum/agoda_com.csv
[dante@machina: ~/code_repos/cloudflare_enum]
->$ cat agoda_com.csv | cut -d "," -f1 | uniq
name
*.agoda.com
agoda.com
analytics.agoda.com
autodiscover.agoda.com
av.agoda.com
connect.agoda.com
deals.agoda.com
hq.agoda.com
meet.agoda.com
partners.agoda.com
```


DEMO TIME

DNS ENUMERATION USING CLOUDFLARE

IANA.ORG SUBDOMAINS

Number of unique subdomains each enumeration technique found independently against iana.org



TALK MATERIAL

<https://github.com/appsecco/bugcrowd-levelup-subdomain-enumeration>

REFERENCES

- <https://www.certificate-transparency.org/>
- <https://www.cloudflare.com/dns/dnssec/how-dnssec-works/>
- <https://www.cloudflare.com/dns/dnssec/dnssec-complexities-and-considerations/>
- https://strotmann.de/roller/dnsworkshop/entry/take_your_dnssec_with_a/
- <https://dnscurve.org/nsec3walker.html>
- <https://github.com/mandatoryprogrammer>
- <https://github.com/rapid7/sonar/wiki/Forward-DNS>
- <https://thehackerblog.com/tag/cloudflare-enumeration/index.html>

About Appsecco

- Pragmatic, holistic, business-focused approach
- Specialist Application Security company
- Highly experienced and diverse team
 - Commercial
 - Security; Gold Standards



OWASP chapter
leads



Certified
Hackers



Assigned
multiple CVEs



Def Con
speakers

THANKS

@yamakira_