INFORMATION SECURITY NEWSPAPER

Type Search Term …

Follow 5,546 followers Like 3.7K YouTube

FIND DETAILS OF ANY MOBILE NUMBER, EMAIL ID, IP ADDRESS IN THE WORLD (STEP BY STEP)

Share this...

OSINT (Open Source Intelligence) is way to collect data from public sources. There are many **tools** & techniques which are capable of gathering information from public sources are the part of **ethical hacking** classes of International Institute of Cyber Security (IICS). Basically before attacking, there is always a need to collect information about your target. So gathering different domains, **sub-domains**, open ports, services & other details. According to ethical hacking researcher of international **institute** of cyber security (IICS), Different search engines such as – shodan, censys are used in scanning/ reconnaissance.

Today we came with another **OSINT** tool which is used in gathering information. It is very common that OSINT tools are used for threat intelligence or cyber investigations. OSINT search Description is an small python script used in extracting data using different search engines & different developers API keys. An python script which is designed to search for public email addresses, domains, phone numbers.

OSINT FUNCTIONALITY OFFERS :-

- Find personal information such as – name, gender, GPS location, age, languages, social network profiles, etc…
- Find information related to data breaches.
- **Find which country a phone number belongs.**
- Find results of google hacking techniques.
- Find results related to domains or an IP addresses.
- Find digital certificates for an certain domain.
- nd CMS for a certain website.
- Find DNS Records and zone transfers information for a certain domain.
- Find Facebook ID and a facebook page full of photos after getting a facebook profile URL.
- Find URLs present in some web page.
- Find URL to know what torrents are being downloaded from some IP.

INSTALLATION OF OSINT SEARCH DESCRIPTION :-

- For testing **Kali Linux 2019.1 amd64** is used. The tool was tested on Live boot of Kali Linux 2019.1 amd64.
- Before installation of OSINT search. Make sure python3 is installed. For installing python type **sudo apt-get update** & **sudo apt-get install python3** As tool runs on python3.
- If python3 is installed. Type **sudo apt-get install python3-dev**

```
root@kali:~/Downloads# apt-get update
 Get:1 http://ftp.yzu.edu.tw/Linux/kali kali-rolling InRelease [30.5 kB]
 Get:2 http://ftp.yzu.edu.tw/Linux/kali kali-rolling/main Sources [12.8 MB]
 e amd64 Packages [187 kB]
 Fetched 30.4 MB in 14s (2,120 kB/s)
 Reading package lists… Done

root@kali:~/Downloads# apt-get install python3
 Reading package lists… Done
```

```
Building dependency tree
Reading state information… Done
The following packages were automatically installed and are no longer required:
  libpython3.6 libpython3.6-dev python3.6-dev
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  libpython3-dev libpython3-stdlib libpython3.7 libpython3.7-dev libpython3.7-minimal libpython3.7-stdlib python3-dev
  python3-distutils python3-minimal python3.7 python3.7-dev python3.7-minimal
Suggested packages:
  python3-doc python3-tk python3-venv python3.7-venv python3.7-doc
The following NEW packages will be installed:
  libpython3.7-dev python3.7-dev
```

- So install pip3 version. For that type **sudo apt-get install python3-pip**
- Type **git clone https://github.com/am0nt31r0/OSINT-Search.git**

```
root@kali:~/Downloads# git clone https://github.com/am0nt31r0/OSINT-Search.git
 Cloning into 'OSINT-Search'…
 remote: Enumerating objects: 30, done.
 remote: Counting objects: 100% (30/30), done.
 remote: Compressing objects: 100% (30/30), done.
 remote: Total 171 (delta 8), reused 0 (delta 0), pack-reused 141
 Receiving objects: 100% (171/171), 61.15 KiB | 279.00 KiB/s, done.
 Resolving deltas: 100% (55/55), done.
```

- Type **cd OSINT-Search** & type **chmod u+x requirements.txt** & type **chmod u+x osintS34rCh.py**
- Type **ls- ltr** for checking permissions.

```
root@kali:~/Downloads# cd OSINT-Search/
root@kali:~/Downloads/OSINT-Search# chmod u+x requirements.txt
root@kali:~/Downloads/OSINT-Search# chmod u+x osintS34rCh.py
root@kali:~/Downloads/OSINT-Search# ls -ltr
 total 52
 -rwxr--r-- 1 root root   145 May  1 05:05 requirements.txt
  rw-r--r-- 1 root root  4317 May  1 05:05 README.md
 -rwxr--r-- 1 root root 40432 May  1 05:05 osintS34rCh.py
```

- Type **pip3 install -r requirements.txt**

```
root@kali:~/Downloads/OSINT-Search# pip3 install -r requirements.txt
 Collecting git+https://github.com/abenassi/Google-Search-API (from -r requirements.txt (line 3))
   Cloning https://github.com/abenassi/Google-Search-API to /tmp/pip-req-build-f4j93eyc
 Collecting validate_email (from -r requirements.txt (line 1))
   Downloading https://files.pythonhosted.org/packages/84/a0/cb53fb64b52123513d04f9b913b905f3eb6fda7264e639b4573cc715c29f/validate_email-1.3.tar.gz
 Collecting opencnam (from -r requirements.txt (line 2))
   Downloading https://files.pythonhosted.org/packages/25/cc/b3bdfedabcf0d0b9b2438dd00d1f65ca8d2d691ba24030cc544a6a0114e8/opencnam-0.6-py3-none-any.whl
 Collecting pyfiglet (from -r requirements.txt (line 4))
   Downloading https://files.pythonhosted.org/packages/33/07/fcfdd7a2872f5b348953de35acce1544dab0c1e8368dca54279b1cde5c15/pyfiglet-0.8.post1-py2.py3-none-any.whl (865kB)
     100% |████████████████████████████████| 870kB 908kB/s
```

- Type **pip3 install git+https://github.com/abenassi/Google-Search-API –upgrade**

```
root@kali:~/Downloads/OSINT-Search# pip3 install git+https://github.com/abenassi/Google-Search-API --upgrade
 Collecting git+https://github.com/abenassi/Google-Search-API
   Cloning https://github.com/abenassi/Google-Search-API to /tmp/pip-req-build-b5sd1rin
 Requirement already satisfied, skipping upgrade: beautifulsoup4 in /usr/lib/python3/dist-packages (from Google-Search-
API==1.1.14) (4.6.3)
 Requirement already satisfied, skipping upgrade: fake-useragent in /usr/local/lib/python3.7/dist-packages (from Google
-Search-API==1.1.14) (0.1.11)
 Requirement already satisfied, skipping upgrade: future in /usr/lib/python3/dist-packages (from Google-Search-API==1.
1.14) (0.15.2)
 Requirement already satisfied, skipping upgrade: requests in /usr/lib/python3/dist-packages (from Google-Search-API==
1.1.14) (2.20.0)
 Requirement already satisfied, skipping upgrade: selenium<3.0.0,>=2.44.0 in /usr/local/lib/python3.7/dist-packages (fr
om Google-Search-API==1.1.14) (2.53.6)
```

- Type **pip3 install https://github.com/PaulSec/API-dnsdumpster.com/archive/master.zip –user**

```
root@kali:~/Downloads/OSINT-Search# pip3 install https://github.com/PaulSec/API-dnsdumpster.com/archive/master.zip --us
er
 Collecting https://github.com/PaulSec/API-dnsdumpster.com/archive/master.zip
   Downloading https://github.com/PaulSec/API-dnsdumpster.com/archive/master.zip
      \ 266kB 21.3MB/s
 Collecting bs4 (from dnsdumpster==0.5)
   Downloading https://files.pythonhosted.org/packages/10/ed/7e8b97591f6f456174139ec089c769f89a94a1a4025fe967691de971f3
14/bs4-0.0.1.tar.gz
 Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from dnsdumpster==0.5) (2.20.0)
```

- Type **python3 osintS34rCh.py**

```
root@kali:~/Downloads/OSINT-Search# python3 osintS34rCh.py
```

```
               _       __   ___________ __ __      _________
  _____  ______(_)____   / /_/  ____/__   // // /  ______/  _____/ /_
 /  __ \/  ___/ /  __ \/  __/\__ \ /_ </ // /_/  ___/ /    /  __ \
/ /_/ (__  ) / / / / /_ ____/ /__/ /__  __/ /   / /___/ / / /
\____/____/_/_/ /_/\__//____/____/  /_/ /_/   \____/_/ /_/
```

```
[-] The following procedure is necessary in order to save your API keys…
 [-] Hit enter if you don't have the keys.
 [-] The data will be written into a file called [/osintSearch.config.ini] that can be edited by you after.
 [?] What is your PIPL API key?
```

- Now from here, enter API keys which are required from the following URLs.
- Create account in each following URLs & copy their APIs into required field of **osintS34rCh.py**

```
https://pipl.com/api
https://www.opencnam.com
https://www.shodan.io
https://whatcms.org/API
https://censys.io/register
https://dashboard.fullcontact.com/consents
```

- After copying type **python3 osintS34rCh.py**

```
[?] What is your PIPL API key?
 gm####################yj9
 [?] What is your FullContact API key?
```

```
Uh###########H9rPOez###########sz
[?] What is your CNAM SID?
AC1#############88d73e0##########
[?] What is your CNAM AUTH_TOKEN?
A#############c403d9############fe5
[?] What is your Shodan API key?
##############wlcjD###################rM
[?] What is your WhatCMS API key?
2###########################ac5376ef9f2d################ce2c40#######d2
[?] What is your Censys API id?
6#######8-####-4723-####-#########bc4e
[?] What is your Censys API secret?
##############2HyMxEOYrY#############
[?] What is your TowerData API key?
c6##################3b09a0############aa8a
```

- Type **python3 osintS34rCh.py -h**

```
root@kali:~/Downloads/OSINT-Search# python3 osintS34rCh.py -h
osintS34rCh v1.0
```

```
 ----------
 ¦USAGES
 ----------
   Email
-----------------------------------------------------------------------------------------------------------------------
   ./osintS34rCh -e                                 # All Searches: Pipl, FullContact, Haveibeenpwnded Data Breaches and
-----------------------------------------------------------------------------------------------------------------------
 Credentials Pastes, TowerData - validate e-mail
---------------------------------------------------------------
   ./osintS34rCh -e  --pipl                         # Pipl
---------------------------------------------------------------

---------
Domain
---------
```

```
   ./osintS34rCh.py -t                                  # All Searches: Shodan Recon, crt.sh, DNSDumpster, All Google
 Hacking Dorks, HackerTarget - DNS Zonetransfer
   ./osintS34rCh.py -t  --shodan                        # Shodan Recon

IP
   ./osintS34rCh.py -t                                      # All Searchs: Shodan and Censys Recon
   ./osintS34rCh.py -t  --shodan                            # Shodan Recon

URL
   ./osintS34rCh.py -u                                     # WhatCMS Check, HackerTarget - Extract URLs
   ./osintS34rCh.py -u  --cms                              # WhatCMS Check

URL
   ./osintS34rCh.py -u                                     # WhatCMS Check, HackerTarget - Extract URLs
   ./osintS34rCh.py -u  --cms                              # WhatCMS Check
```

FIND EMAIL IDS

- Type **python3 osintS34rCh.py -e abh#########a6##@gmail.com –pwned**
- **-e** is used to search information about emails.
- **abh#########a6##@gmail.com** is the target email id. For security we have hide the email id and as this email ID is created specifically for **cyber forensics** classes of International Institute of Cyber Security.
- **–pwned** is query to search for if there is any data breach.

```
root@kali:~/Downloads/OSINT-Search# python3 osintS34rCh.py -e abh##########a6##@gmail.com --pwned
```

```
                _       __   __________ __ __      _________
  ____   _____(_)___   / /_/ ___/__   // // / ______/ _____/ /_
```

```
 / __ \/ ___/ / __ \/ __/\__ \ /_ </ // /_/ ___/ /   / __ \
/ /_/ (__  ) / / / / /_ ___/ / __/ /__  __/ /  / /___/ / / /
\____/____/_/_/ /_/\__//____/____/  /_/ /_/   \____/_/ /_/
```

```
-> Data Breaches Results
 [@] Target: abh###########a6##@gmail.com
 ] Data breach: Digimon [] Title: Digimon
 [] Domain: digimon.co.in [] Date of the breach: 2016-09-05
 [] Number of accounts breached: 7687679 [] Description: In September 2016, over 16GB of logs from a service indicated
 to be digimon.co.in were obtained, most likely from an unprotected Mongo DB instance. The service ceased running short
ly afterwards and no information remains about the precise nature of it. Based on enquiries made via Twitter, it appear
s to have been a mail service possibly based on PowerMTA and used for delivering spam. The logs contained information i
ncluding 7.7M unique email recipients (names and addresses), mail server IP addresses, email subjects and tracking info
rmation including mail opens and clicks.
 [] Logo image from Digimon: https://haveibeenpwned.com/Content/Images/PwnedLogos/Email.png [] Data breached: Email add
resses
 [] Data breached: Email messages [] Data breached: IP addresses
 [*] Data breached: Names
 [] Data breach: Dubsmash [] Title: Dubsmash
 [] Domain: dubsmash.com [] Date of the breach: 2018-12-01
 [] Number of accounts breached: 161749950 [] Description: In December 2018, the video messaging service Dubsmash suffe
red a data breach. The incident exposed 162 million unique email addresses alongside usernames and PBKDF2 password hash
es. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and
 subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attribut
ed to "BenjaminBlue@exploit.im".
 [] Logo image from Dubsmash: https://haveibeenpwned.com/Content/Images/PwnedLogos/Dubsmash.png [] Data breached: Email
 addresses
 [] Data breached: Geographic locations [] Data breached: Names
 [] Data breached: Passwords [] Data breached: Phone numbers
 [] Data breached: Spoken languages [] Data breached: Usernames
 [] Data breach: MySpace [] Title: MySpace
 [] Domain: myspace.com [] Date of the breach: 2008-07-01
 [] Number of accounts breached: 359420698 [] Description: In approximately 2008, MySpace suffered a data breach that e
xposed almost 360 million accounts. In May 2016 the data was offered up for sale on the "Real Deal" dark market website
and included email addresses, usernames and SHA1 hashes of the first 10 characters of the password converted to lowerc
ase and stored without a salt. The exact breach date is unknown, but analysis of the data suggests it was 8 years befor
e being made public.
 [] Logo image from MySpace: https://haveibeenpwned.com/Content/Images/PwnedLogos/MySpace.png [] Data breached: Email a
ddresses
 [] Data breached: Passwords [] Data breached: Usernames
 [] Data breach: Tumblr [] Title: tumblr
 [] Domain: tumblr.com [] Date of the breach: 2013-02-28
 [] Number of accounts breached: 65469298 [] Description: In early 2013, tumblr suffered a data breach which resulted i
n the exposure of over 65 million accounts. The data was later put up for sale on a dark market website and included em
ail addresses and passwords stored as salted SHA1 hashes.
 [] Logo image from Tumblr: https://haveibeenpwned.com/Content/Images/PwnedLogos/Tumblr.png [] Data breached: Email add
resses
 [*] Data breached:Passwords
```

- Above output shows, there are 3 data breached with above email id. First one is the **DUBMASH** messaging application.
- An video messaging application experienced data breach in December 2018 with over 162 millions of emails. Later on data containing usernames & password hashes were sold on dark web.
- Second is an way old but effective data breach on **Myspace**. Myspace is popular social networking site offers photos, music, video, user submission of network friends. As per above data breach, this site data was also found on sale in REAL DARK website. Including usernames, passwords hashes, addresses.
- Third is **Tumblr** breach where it was suffered of data breach around 65 million which was on sale on dark market.

FIND HOSTS, PUBLIC KEYS OF TARGET

- Type **python3 osintS34rCh.py -t certifiedhacker.com**
- **-t** is used for searching information related to domain.
- **certifiedhacker.com** is target site.

```
ot@kali:~/Downloads/OSINT-Search# python3 osintS34rCh.py -t certifiedhacker.com
```

```
                 _          __  ______________ __ __        __________
  ____  _______(_)___    / /_/ ___/__  // // / ______/ _____/ /_
 / __ \/ ___/ / __ \/ __/\__ \ /_ </ // /_/ ___/ /    / __ \
/ /_/ (__  ) / / / / /_ ___/ / /__/ /__  __/ /  / /____/ / / /
\____/_____/_/_/ /_/\__//_____/_____/  /_/ /_/   \____/_/ /_/
```

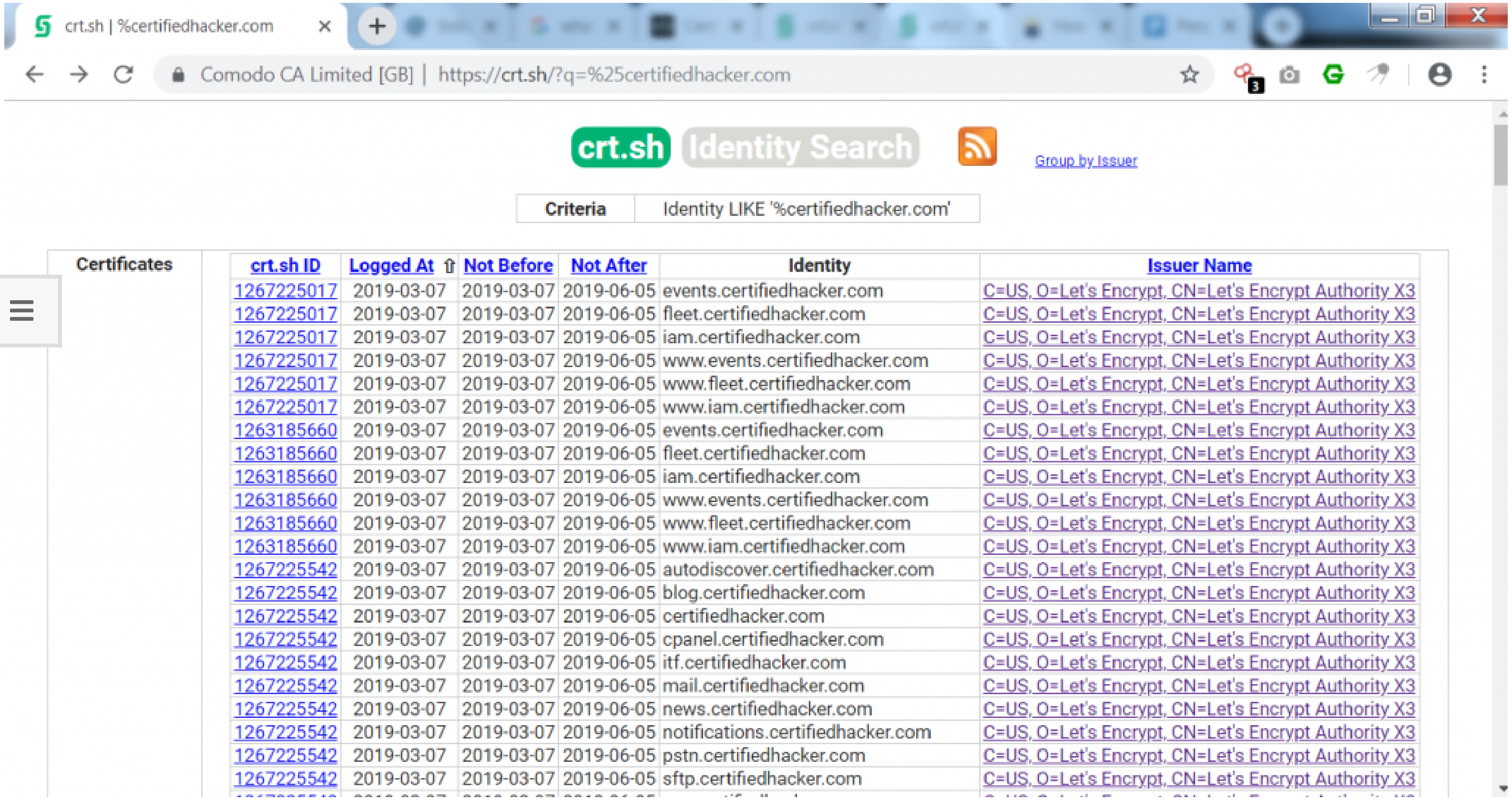
```
-> Shodan Results
 -> Shodan Results
 [@] Target: certifiedhacker.com
 [!] Shodan: information about certifiedhacker.com was not found.

 -> CRT.sh Results
 [@] Target: certifiedhacker.com
 [-] URL: https://crt.sh/?q=%25certifiedhacker.com
 [] Issuer CA ID: 16418 [] Issuer Name: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
 [] Name: events.certifiedhacker.com [] Logged At: 2019-03-07T17:07:30.61
 [] Not before: 2019-03-07T16:07:29 [] Not after: 2019-06-05T16:07:29
 [] Issuer CA ID: 16418 [] Issuer Name: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
 [] Name: fleet.certifiedhacker.com [] Logged At: 2019-03-07T17:07:30.61
 [] Not before: 2019-03-07T16:07:29 [] Not after: 2019-06-05T16:07:29
```

```
  [] Issuer CA ID: 16418 [] Issuer Name: C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
  [] Name: iam.certifiedhacker.com [] Logged At: 2019-03-07T17:07:30.61
  [] Not before: 2019-03-07T16:07:29 [] Not after: 2019-06-05T16:07:29

-> DNSdumpster Results
  [@] Target: certifiedhacker.com
   *] DNS Servers
  Domain: ns2.bluehost.com.
  IP: 162.159.25.175
  Reverse DNS: ns2.bluehost.com
  AS: AS13335
  ISP: Cloudflare Inc
  Country: United States
  Header:
  Domain: ns1.bluehost.com.
  IP: 162.159.24.80
  Reverse DNS: ns1.bluehost.com
  AS: AS13335
  ISP: Cloudflare Inc
  Country: United States
  Header:
  [*] MX Records
  Domain: 0 mail.certifiedhacker.com.
  IP: 162.241.216.11
  Reverse DNS: box5331.bluehost.com
  AS: AS20013
  ISP: CyrusOne LLC
  Country: United States
```

```
Header: mail.certifiedhacker.com.
[*] TXT Records
"v=spf1 a mx ptr include:bluehost.com ?all"
[*] Host Records
Domain: soc.certifiedhacker.com
IP: 162.241.216.11
Reverse DNS: box5331.bluehost.com
AS: AS20013
ISP: CyrusOne LLC
Country: United States
Header: nginx/1.12.2HTTPS: nginx/1.12.2FTP: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------//220-You are
user number 1 of 150 allowed.//220-Local time is now 23:54. Server port: 21.//220-IPv6 connections are also welcome on
this server.//220 You will be disconnected after 15 minutes of inactivity.//SSH: SSH-2.0-OpenSSH_5.3TCP8080: nginx/1.1
2.2
Domain: www.soc.certifiedhacker.com
IP: 162.241.216.11
Reverse DNS: box5331.bluehost.com
AS: AS20013
ISP: CyrusOne LLC
Country: United States
Header: nginx/1.12.2HTTPS: nginx/1.12.2FTP: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------//220-You are
user number 1 of 150 allowed.//220-Local time is now 23:54. Server port: 21.//220-IPv6 connections are also welcome on
this server.//220 You will be disconnected after 15 minutes of inactivity.//SSH: SSH-2.0-OpenSSH_5.3TCP8080: nginx/1.1
2.2
Domain: itf.certifiedhacker.com
IP: 162.241.216.11
Reverse DNS: box5331.bluehost.com
AS: AS20013
```

```
ISP: CyrusOne LLC
Country: United States
Header: nginx/1.12.2HTTPS: nginx/1.12.2FTP: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------//220-You are user number 1 of 150 allowed.//220-Local time is now 23:54. Server port: 21.//220-IPv6 connections are also welcome on this server.//220 You will be disconnected after 15 minutes of inactivity.//SSH: SSH-2.0-OpenSSH_5.3TCP8080: nginx/1.12.2

-> Zone Transfer Results
; <<>> DiG 9.11.3-1ubuntu1.7-Ubuntu <<>> axfr @ns2.bluehost.com certifiedhacker.com
; (1 server found)
;; global options: +cmd
; Transfer failed.
; <<>> DiG 9.11.3-1ubuntu1.7-Ubuntu <<>> axfr @ns1.bluehost.com certifiedhacker.com
; (1 server found)
;; global options: +cmd
; Transfer failed.
```

- Above output shows shodan was unable to find everything about target site. Then Crt.sh find the URLs same as target site. Crt.sh shows the domains & sub-domains of target website. Crt.sh (Certificate Transparency) is developed to increase security of public key.
- When we open the first link from crt.sh. It shows associated links same as target site(certified hacker.com)

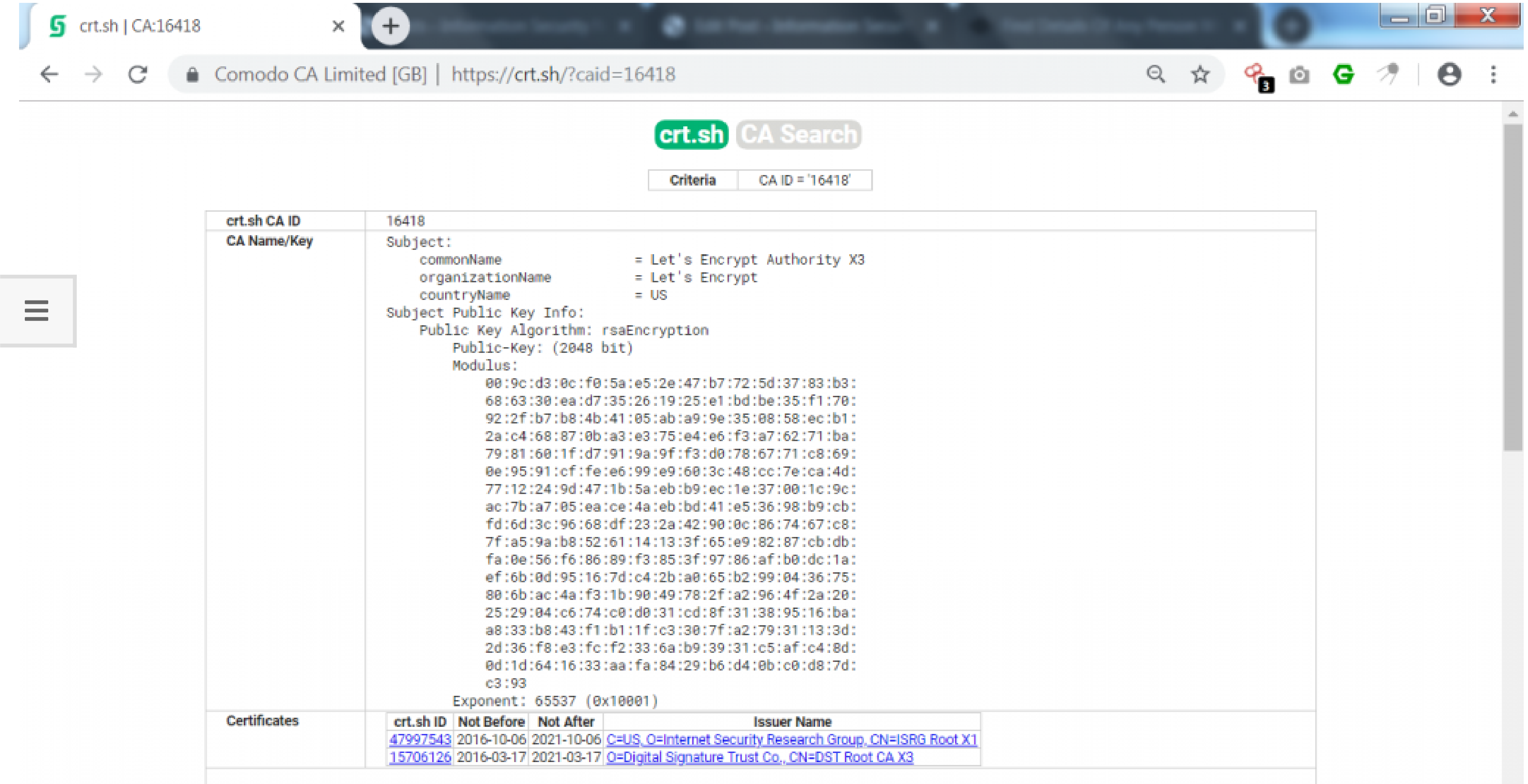

crt.sh | %certifiedhacker.com
Comodo CA Limited [GB] | https://crt.sh/?q=%25certifiedhacker.com
crt.sh Identity Search
Group by Issuer

Criteria	Identity LIKE '%certifiedhacker.com'

Certificates

crt.sh ID	Logged At ⇧	Not Before	Not After	Identity	Issuer Name
1267225017	2019-03-07	2019-03-07	2019-06-05	events.certifiedhacker.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1267225017	2019-03-07	2019-03-07	2019-06-05	fleet.certifiedhacker.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1267225017	2019-03-07	2019-03-07	2019-06-05	iam.certifiedhacker.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1267225017	2019-03-07	2019-03-07	2019-06-05	www.events.certifiedhacker.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1267225017	2019-03-07	2019-03-07	2019-06-05	www.fleet.certifiedhacker.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1267225017	2019-03-07	2019-03-07	2019-06-05	www.iam.certifiedhacker.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1263185660	2019-03-07	2019-03-07	2019-06-05	events.certifiedhacker.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1263185660	2019-03-07	2019-03-07	2019-06-05	fleet.certifiedhacker.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1263185660	2019-03-07	2019-03-07	2019-06-05	iam.certifiedhacker.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1263185660	2019-03-07	2019-03-07	2019-06-05	www.events.certifiedhacker.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1263185660	2019-03-07	2019-03-07	2019-06-05	www.fleet.certifiedhacker.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1263185660	2019-03-07	2019-03-07	2019-06-05	www.iam.certifiedhacker.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1267225542	2019-03-07	2019-03-07	2019-06-05	autodiscover.certifiedhacker.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1267225542	2019-03-07	2019-03-07	2019-06-05	blog.certifiedhacker.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1267225542	2019-03-07	2019-03-07	2019-06-05	certifiedhacker.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1267225542	2019-03-07	2019-03-07	2019-06-05	cpanel.certifiedhacker.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1267225542	2019-03-07	2019-03-07	2019-06-05	itf.certifiedhacker.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1267225542	2019-03-07	2019-03-07	2019-06-05	mail.certifiedhacker.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1267225542	2019-03-07	2019-03-07	2019-06-05	news.certifiedhacker.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1267225542	2019-03-07	2019-03-07	2019-06-05	notifications.certifiedhacker.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1267225542	2019-03-07	2019-03-07	2019-06-05	pstn.certifiedhacker.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1267225542	2019-03-07	2019-03-07	2019-06-05	sftp.certifiedhacker.com	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

- Above link shows same link as like certifiedhacker.com. Opening first link shows the public key of URL with the common name of Let’s encrypt authority.



Criteria	CA ID = '16418'

crt.sh CA ID	16418

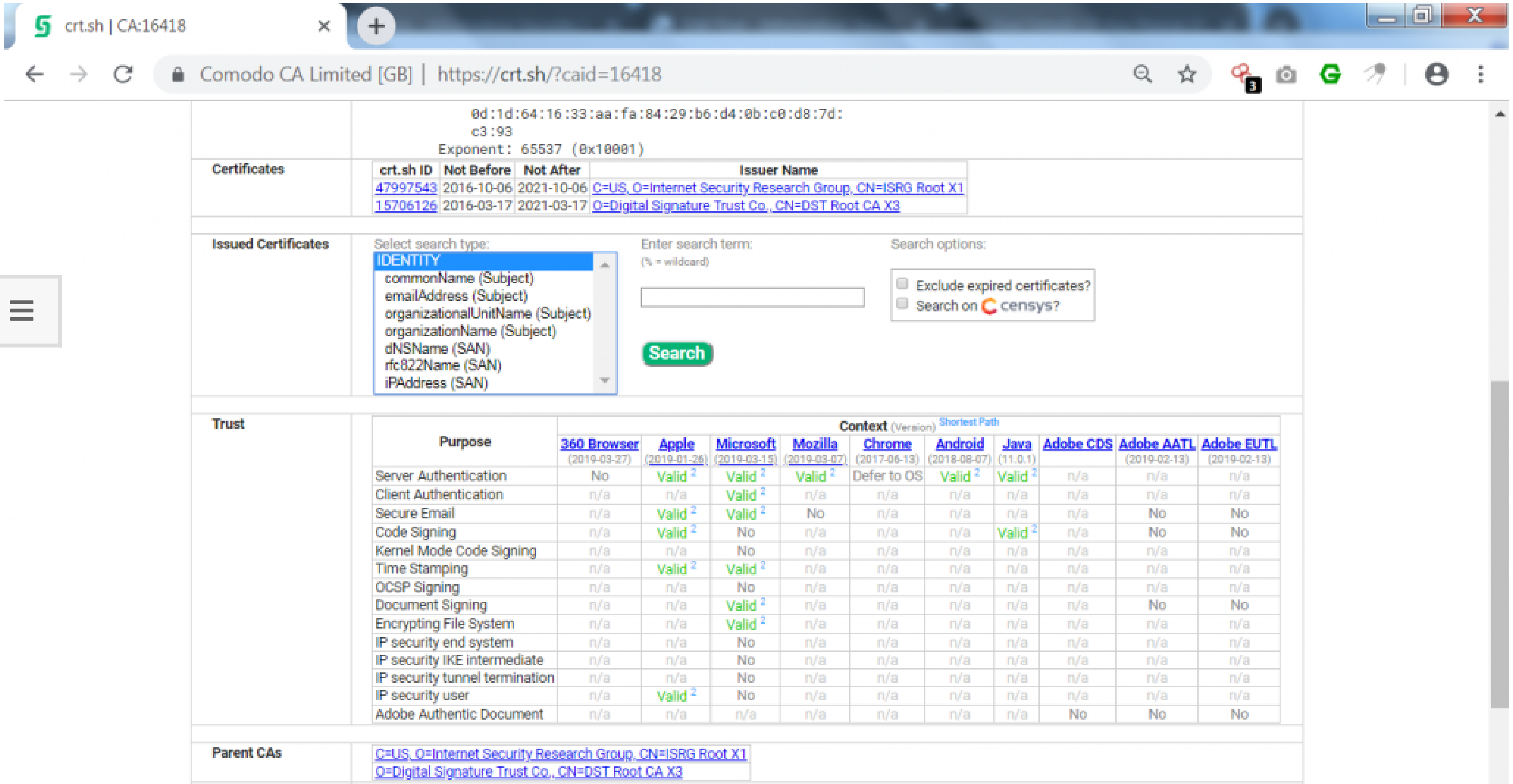
CA Name/Key

```
Subject:
    commonName                = Let's Encrypt Authority X3
    organizationName          = Let's Encrypt
    countryName               = US
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
        Public-Key: (2048 bit)
        Modulus:
            00:9c:d3:0c:f0:5a:e5:2e:47:b7:72:5d:37:83:b3:
            68:63:30:ea:d7:35:26:19:25:e1:bd:be:35:f1:70:
            92:2f:b7:b8:4b:41:05:ab:a9:9e:35:08:58:ec:b1:
            2a:c4:68:87:0b:a3:e3:75:e4:e6:f3:a7:62:71:ba:
            79:81:60:1f:d7:91:9a:9f:f3:d0:78:67:71:c8:69:
            0e:95:91:cf:fe:e6:99:e9:60:3c:48:cc:7e:ca:4d:
            77:12:24:9d:47:1b:5a:eb:b9:ec:1e:37:00:1c:9c:
            ac:7b:a7:05:ea:ce:4a:eb:bd:41:e5:36:98:b9:cb:
            fd:6d:3c:96:68:df:23:2a:42:90:0c:86:74:67:c8:
            7f:a5:9a:b8:52:61:14:13:3f:65:e9:82:87:cb:db:
            fa:0e:56:f6:86:89:f3:85:3f:97:86:af:b0:dc:1a:
            ef:6b:0d:95:16:7d:c4:2b:a0:65:b2:99:04:36:75:
            80:6b:ac:4a:f3:1b:90:49:78:2f:a2:96:4f:2a:20:
            25:29:04:c6:74:c0:d0:31:cd:8f:31:38:95:16:ba:
            a8:33:b8:43:f1:b1:1f:c3:30:7f:a2:79:31:13:3d:
            2d:36:f8:e3:fc:f2:33:6a:b9:39:31:c5:af:c4:8d:
            0d:1d:64:16:33:aa:fa:84:29:b6:d4:0b:c0:d8:7d:
            c3:93
        Exponent: 65537 (0x10001)
```

Certificates

crt.sh ID	Not Before	Not After	Issuer Name
47997543	2016-10-06	2021-10-06	C=US, O=Internet Security Research Group, CN=ISRG Root X1
15706126	2016-03-17	2021-03-17	O=Digital Signature Trust Co., CN=DST Root CA X3

SNIP



crt.sh | CA:16418

Comodo CA Limited [GB] | https://crt.sh/?caid=16418

```
                    0d:1d:64:16:33:aa:fa:84:29:b6:d4:0b:c0:d8:7d:
                    c3:93
                Exponent: 65537 (0x10001)
```

Certificates

crt.sh ID	Not Before	Not After	Issuer Name
47997543	2016-10-06	2021-10-06	C=US, O=Internet Security Research Group, CN=ISRG Root X1
15706126	2016-03-17	2021-03-17	O=Digital Signature Trust Co., CN=DST Root CA X3

Issued Certificates

Select search type:
IDENTITY
commonName (Subject)
emailAddress (Subject)
organizationalUnitName (Subject)
organizationName (Subject)
dNSName (SAN)
rfc822Name (SAN)
iPAddress (SAN)

Enter search term:
(% = wildcard)

Search options:
□ Exclude expired certificates?
□ Search on censys?

Search

Trust

Purpose	Context (Version) Shortest Path									
	360 Browser (2019-03-27)	Apple (2019-01-26)	Microsoft (2019-03-15)	Mozilla (2019-03-07)	Chrome (2017-06-13)	Android (2018-08-07)	Java (11.0.1)	Adobe CDS	Adobe AATL (2019-02-13)	Adobe EUTL (2019-02-13)
Server Authentication	No	Valid [2]	Valid [2]	Valid [2]	Defer to OS	Valid [2]	Valid [2]	n/a	n/a	n/a
Client Authentication	n/a	n/a	Valid [2]	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Secure Email	n/a	Valid [2]	Valid [2]	No	n/a	n/a	n/a	n/a	No	No
Code Signing	n/a	Valid [2]	No	n/a	n/a	n/a	Valid [2]	n/a	No	No
Kernel Mode Code Signing	n/a	n/a	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Time Stamping	n/a	Valid [2]	Valid [2]	n/a	n/a	n/a	n/a	n/a	n/a	n/a
OCSP Signing	n/a	n/a	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Document Signing	n/a	n/a	Valid [2]	n/a	n/a	n/a	n/a	n/a	No	No
Encrypting File System	n/a	n/a	Valid [2]	n/a	n/a	n/a	n/a	n/a	n/a	n/a
IP security end system	n/a	n/a	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a
IP security IKE intermediate	n/a	n/a	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a
IP security tunnel termination	n/a	n/a	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a
IP security user	n/a	Valid [2]	No	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Adobe Authentic Document	n/a	n/a	n/a	n/a	n/a	n/a	n/a	No	No	No

Parent CAs

C=US, O=Internet Security Research Group, CN=ISRG Root X1
O=Digital Signature Trust Co., CN=DST Root CA X3

- Further it shows issued certificates on the URL. Then it shows authentication of URL. Valid shows that browser has passed the authentication on every purposes.
- Most of URLs in crt.sh shows same authentications.
- **DNSdumpster** is designed to search for discovered hosts related to domains. DNSdumpster find all the visible hosts for the attackers.
- In the above output, Dnsdumpster has gather 5 host records & other domains of target site. There are numerous way to gather hosts of any domain. We have shown how **NSLOOKUP** is used in gathering different hosts.
- Then it shows the different domains of target site containing reverse dns, country, IP address, ISP & header of dns.
- Above output of OSINT search has gathered different records which can be used in further scanning methods.
- Then it shows name of the server in zone transfer but was unable to transfer any part of the file.

FINDING OPEN PORTS

- Type **python3 osintS34rCh.py -t 162.241.216.11**
- **-t** is used to enter IP address.
- **162.241.216.11** is the target IP address.

```
root@kali:~/Downloads/OSINT-Search# python3 osintS34rCh.py -t 162.241.216.11
```

```
  ---------------------------------------------------------
                _      __  __________ __ __       ________
  =========================================================
  ____  _____(_)___   / /_/ ____/__  // // /  _____/  ____/ /_
===========================================================
 / __ \/ ___/ / __ \/ __/\__ \ /_ </ // /_/ ___/ /   / __ \
===========================================================
/ /_/ (__  ) / / / / /_ ___/ /__/ /__  __/ /  / /___/ / / /
===========================================================
\____/____/_/_/ /_/\__//____/____/   /_/ /_/   \____/_/ /_/
-----------------------------------------------------------
```

```
-> Shodan Results
 [@] Target: 162.241.216.11
 [] City: Provo [] Country: United States
 [] Postal Code: 84606 [] Longitude: -111.6133
 [] Latitude: 40.21809999999999 [] Operation System: None
 [] Organization: CyrusOne LLC [] ISP: Unified Layer
 [] Port: 465 [] Port: 443
 [] Port: 2096 [] Port: 8080
 [] Port: 995 [] Port: 993
 [] Port: 22 [] Port: 587
 [] Port: 53 [] Port: 25
 [] Port: 80 [] Port: 2222
 [] Port: 2087 [] Port: 5432
 [] Port: 2082 [] Port: 2083
 [] Port: 26 [] Hostname: box5331.bluehost.com
 -> Censys Results
 [] IP: 162.241.216.11 [] Protocol: 80/http
 [] Protocol: 3306/mysql [] Protocol: 8080/http
 [] Protocol: 993/imaps [] Protocol: 465/smtp
 [] Protocol: 995/pop3s [] Protocol: 110/pop3
 [] Protocol: 21/ftp [] Protocol: 143/imap
 [] Protocol: 53/dns [] Protocol: 587/smtp
 [] Protocol: 443/https [] Protocol: 22/ssh
 [] Protocol: 5432/postgres [] Country: United States
 [] Registered Country: United States [] Longitude: -111.6442
 [] Latitude: 40.2342 [] Continent: North America
 [] Timezone: America/Denver [] AS Name: UNIFIEDLAYER-AS-1 - Unified Layer
 [] AS Country Code: US [] AS Description: UNIFIEDLAYER-AS-1 - Unified Layer

 [] Service: https/443 [] Certificate DNS Names: ['.bluehost.com', 'bluehost.com'] [] Issued By: {'common_name': ['COMODO RSA Domain Validation Secure Server CA'], 'country': ['GB'], 'locality': ['Salford'], 'province': ['Greater Manchester'], 'organization': ['COMODO CA Limited']}
 [] Service: dns/53 [] Open Resolver: True
 [*] Lookup Answers: {'type': 'A', 'name': 'c.afekv.com', 'response': '162.241.216.11'}

 [*] Updated at: 2019-05-01T08:18:45+00:00
```

- Above output shows open ports from shodan containing registered country with longitude & latitude.
- Shodan has found open ports of target site. Some ports which are found with common vulnerability can be used in further footprinting methods.
- Censys has also found common listed ports which are used in information gathering methods.
- These all techniques are the curriculum of **ethical hacking** classes of International Institute of Cyber Security.

EXTRACTING URLS

- Type **python3 osintS34rCh.py -u certifiedhacker.com**
- **-u** is used to enter domain name.
- **certifiedhacker.com** is target domain name.

```
root@kali:~/Downloads/OSINT-Search# python3 osintS34rCh.py -u certifiedhacker.com
```

```
  --------------------------------------------------------
                _      __  __________ __ __      ________
  ========================================================
  ____  _____(_)___   / /_/ ___/__   // // / _____/ _____/ /_
===========================================================
 /  __ \/ ___/ /  __ \/  __/\__ \ /_ </ // /_/ ___/ /   /  __ \
===========================================================
/ /_/ (__  ) / / / / /_ ___/ /__/ /__  __/ /  / /___/ / / /
===========================================================
\____/____/_/_/ /_/\__//____/____/  /_/ /_/   \____/_/ /_/
-----------------------------------------------------------
```

```
-> Extract URLs Results
 Visible links
 http://certifiedhacker.com/
 http://certifiedhacker.com/images/icons/lock-and-key-110.png
 http://certifiedhacker.com/
 http://certifiedhacker.com/sample-login.html
 http://certifiedhacker.com/P-folio/index.html
 http://certifiedhacker.com/images/slideshow/slide-1.png
 http://certifiedhacker.com/Online Booking/index.htm
 http://certifiedhacker.com/images/slideshow/slide-2.png
 http://certifiedhacker.com/corporate-learning-website/01-homepage.html
 http://certifiedhacker.com/images/slideshow/slide-3.png
 http://certifiedhacker.com/Real Estates/index.html
 http://certifiedhacker.com/images/slideshow/slide-4.png
 http://certifiedhacker.com/Recipes/index.html
 http://certifiedhacker.com/images/slideshow/slide-5.png
```

```
http://certifiedhacker.com/Social Media/index.html
http://certifiedhacker.com/images/slideshow/slide-6.png
http://certifiedhacker.com/Turbo Max/index.htm
http://certifiedhacker.com/images/slideshow/slide-7.png
http://certifiedhacker.com/Under Construction/index.html
http://certifiedhacker.com/images/slideshow/slide-8.png
http://certifiedhacker.com/Under the trees/index.html
http://certifiedhacker.com/images/slideshow/slide-9.png
http://certifiedhacker.com/
```

- After scanning with URL query, OSINT-search has gather all the links of target site. The above link can be used in further footprinting methods.

FINDING DETAILS OF MOBILE NUMBERS

- Type **python3 osintS34rCh.py -p +919####677## –callerID**
- **-p** is used for to enter phone number, **–callerID** is the query.
- **+919####677##** is target mobile number. For security, mobile number is hidden. Mobile number forensics is the essential topic of cyber forensics classes of International Institute of Cyber Security

```
root@kali:~/Downloads/OSINT-Search# python3 osintS34rCh.py -p +918071992699 --callerID
```

```
                _       __  ______________ __ __      ________
  _____ ______(_)___   / /_/ ____/__  // // / ______/ _____/ /_
 / __ \/ ___/ / __ \/ __/\__ \ /_ </ // /_/ ____/ /   / __ \
/ /_/ (__  ) / / / / /_ ____/ /__/ /__  __/ /   / /___/ / / /
\____/____/_/_/ /_/\__//____/____/  /_/ /_/    \____/_/ /_/
```

```
-> Caller ID Results
 [] Number: +919####677## [] Country: DELHI IN
```

- Above output shows current location of mobile number. Output can be used in initial phase of footprinting/ reconnaissance method.
- Type **python3 osintS34rCh.py -p +919####254## –callerID**
- **-p** is used for to enter phone number, **–callerID** is the query.
- **19####254##** is target mobile number. For security, mobile number is hidden.

```
root@kali:~/Downloads/OSINT-Search# python3 osintS34rCh.py -p +919####254##  --callerID
```

```
               _       __  __________ __ __       ________
  ____  _____(_)___  / /_/ ___/__  // // / _____/ ____/ /_
 / __ \/ ___/ / __ \/ __/\__ \ /_ </ // /_/ ___/ /   / __ \
/ /_/ (__  ) / / / / /_ ___/ /__/ /__  __/ /  / /___/ / / /
\____/____/_/_/ /_/\__//____/____/  /_/ /_/   \____/_/ /_/
```

```
-> Caller ID Results
 [] Number: +919####254## [] Country: DELHI IN
```

- Above output shows current location of mobile number. Output can be used in initial phase of footprinting/ reconnaissance method.
- Type **python3 osintS34rCh.py -p +52#########78 –callerID**
- **-p** is used for to enter phone number. **–callerID** is the query.
- **+52#########78** is target mobile number. For security, mobile number is hidden.

```
root@kali:~/Downloads/OSINT-Search# python3 osintS34rCh.py -p+52#########78  --callerID
```

```
               _       __  __________ __ __       ________
  ____  _____(_)___  / /_/ ___/__  // // / _____/ ____/ /_
```

```
 / __ \/ ___/ / __ \/ __/\__ \ /_ </ // /_/ ___/  /   / __ \
/ /_/ (__  ) / / / / /_ ___/ /__/ /__  __/ /  / /___/ / / /
\____/____/_/_/ /_/\__//____/____/  /_/ /_/   \____/_/ /_/
```

```
-> Caller ID Results
 [] Number: +52#########78 [] Country: VARRERA
```

- Above output shows current location of mobile number. Output can be used in initial phase of footprinting/ reconnaissance method.
- Type **python3 osintS34rCh.py -p +52########02 –callerID**
- **-p** is used for to enter phone number. **–callerID** is the query.
- **+52########02** is target mobile number. For security, mobile number is hidden.

```
root@kali:~/Downloads/OSINT-Search# python3 osintS34rCh.py -p +52########02 --callerID
```

```
            _           __  _______ __ __      ______
  ____  _____(_)___   / /_/ ___/__  // // /  _____/ ____/ /_
 / __ \/ ___/ / __ \/ __/\__ \ /_ </ // /_/ ___/  /   / __ \
/ /_/ (__  ) / / / / /_ ___/ /__/ /__  __/ /  / /___/ / / /
\____/____/_/_/ /_/\__//____/____/  /_/ /_/   \____/_/ /_/
```

```
-> Caller ID Results
 [] Number: +52########02  [] Country: MIGUEL HIDAL MX
```

- Above output shows current location of mobile number. Output can be used in initial phase of foot printing/ **reconnaissance** method.
- Any unsuspected number can be checked that from which country it belongs.

(Visited 1,047 1 times)

Share this...

BY: JIM GILL / ON: MAY 2, 2019 / IN: RECONNAISSANCE, SCANNING, TUTORIALS / TAGGED: GATHER INFORMATION WITH OSINT, OSINT SEARCH QUERY, OSINT SEARCH USING
, OSINT-SEARCH, OSINT-SEARCH TECHNIQUES

FOLLOW & LIKE US

Follow Like

LATEST VIDEOS

POPULAR NEWS VIDEO 12 JULY

POPULAR NEWS VIDEO 11 JULY

VIEW ALL

POPULAR POSTS

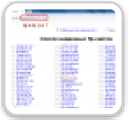
HOW TO EXPLOIT NEW FACEBOOK FEATURE TO ACCESS…

HOW TO HACK WI-FI: CRACKING WPA2-PSK PASSWORDS USING…

HOW TO FAKE YOUR PHONE NUMBER: MAKE IT LOOK LIKE…

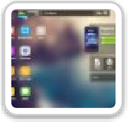
HOW TO INTERCEPT MOBILE COMMUNICATIONS (CALLS AND…

HOW TO SCAN WHOLE INTERNET 3.7 BILLION IP ADDRESSES…

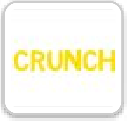


LIST OF ALL OPEN FTP SERVERS IN THE WORLD

CRACK WINDOWS PASSWORD WITH JOHN THE RIPPER

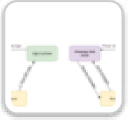


HOW TO CONNECT ANDROID TO PC/MAC WITHOUT WIFI



CREATE YOUR OWN WORDLIST WITH CRUNCH

HOW TO EXPLOIT SUDO VIA LINUX PRIVILEGE ESCALATION

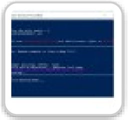


HIJACKING WHATSAPP ACCOUNTS USING WHATSAPP WEB

FIND WEBCAMS, DATABASES, BOATS IN THE SEA USING SHODAN

HACK WHATSAPP ACCOUNT OF YOUR FRIEND

DO HACKING WITH SIMPLE PYTHON SCRIPT



EXTRACTING HASHES & PLAINTEXT PASSWORDS FROM WINDOWS 10

FAKE ANY WEBSITE IN SECONDS FACEBOOK, SNAPCHAT, INSTAGRAM :-

HOW TO HACK ANY CAR WITH THIS TOOL

HACK WINDOWS, ANDROID, MAC USING THEFATRAT (STEP BY…

BEST HACKING TOOLS OF 2017 FOR WINDOWS, LINUX, AND OS X

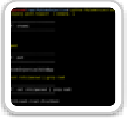
HACKSPY TROJAN EXPLOIT

BYPASS ANTIVIRUS DETECTION WITH PHANTOM PAYLOADS

HACK ANY WEBSITE WITH ALL IN ONE TOOL

PORNHUB AND ITS METHOD TO BYPASS INDIA’S PORN SITES BAN

PIRATED SMASH BROS. ULTIMATE COPY FOR SALE IN MEXICO…

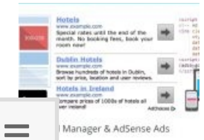


EXPLOITING PYTHON CODE INJECTION IN WEB APPLICATIONS

VULNERABILITIES

CRITICAL VULNERABILITY IN SIEMENS’ INDUSTRIAL CONTROL SYSTEM

IOMEGA STORCENTER & LENOVO EMC NAS DEVICES ARE LEAKING USERS’ INFORMATION



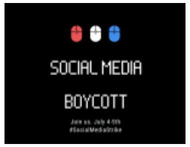
AD INSERTER, A WORDPRESS PLUGIN, ALLOWS REMOTE CODE EXECUTION

NEW IOS 13 VULNERABILITY ALLOWS ACCESS TO PASSWORDS STORED ON YOUR IPHONE

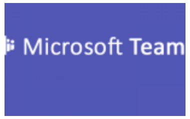
NEW EXPLOIT ALLOWS HACKERS TO ACCESS SHARED FILES VIA WHATSAPP AND TELEGRAM

INTEL DATA CENTER SSD DRIVES ALLOW HACKERS TO TAKE COMPLETE CONTROL OF SERVERS

APPLE WATCH VULNERABILITY ALLOWS YOU TO SPY ON YOUR FRIENDS’ IPHONE



THIS PGP BUG COULD ALLOW HACKERS TO CONTROL YOUR EMAIL SERVERS



VULNERABILITY IN MICROSOFT TEAMS COULD ALLOW HACKER TO GAIN COMPLETE CONTROL OF YOUR INFRASTRUCTURE

ORIGIN, AN EA PLATFORM, EXPOSES DATA OF 300 MILLION USERS

FAKE EMERGENCY ALERTS ARE LAUNCHED VIA VULNERABILITY IN LTE

A HACKER PUBLISHED A NEW IOS JAILBREAK13 WITH TFP0 EXPLOIT

DELL LAPTOPS ARE NOT SECURE; ANOTHER VULNERABILITY IN DELL SOFTWARE

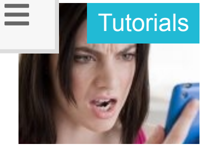
CISCO DNA ALLOWED UNAUTHORIZED USERS ACCESS TO ENTERPRISE NETWORKS FOR A LONG TIME

ANOTHER ZERO DAY FOUND IN MOZILLA FIREFOX IT’S CAUSING UNREST AMONG TOR USERS

CREATE WINDOWS 10 FUD (FULLY UNDETECTABLE) PAYLOAD

VIEW ALL

TUTORIALS



HOW TO CHECK IF YOUR MOBILE PHONE IS HACKED OR NOT?

CHECK IF YOUR WHATSAPP IS HACKED OR NOT ?

HOW TO ANALYZE USB TRAFFIC

HOW DO YOU CHECK THAT A WEBSITE IS UNSAFE?

Configuring update for Windows 10
5% complete
Do not turn off your computer
ble Windows 10 Updates & Defen

HAVING PROBLEM WITH WINDOWS 10 UPDATES? DISABLE IN 2 MINUTES

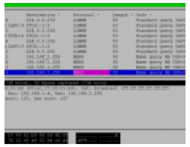
CREATE WINDOWS 10 FUD (FULLY UNDETECTABLE) PAYLOAD

HOW TO OPEN UNKNOWN FILES THAT HAVE MALWARE IN WINDOWS 10 WITH SANDBOX

KILLSHOT TO HACK ANY WEBSITE

TALK SECRETLY WITH YOUR FRIENDS – EVERYTHING ABOUT STEGANOGRAPHY

SOLUTION TO SPAMMING, CHECK ANY UNKNOWN EMAIL ID EXISTENCE

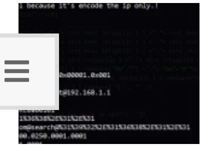


LIGHT WEIGHT PACKETS ANALYZER IS HERE!

SMART WAY OF DISCOVERING COMPUTER ON NETWORK USING ARPING

TOP 5 TOOLS USED BY CYBER CRIMINALS RECENTLY

FIND DETAILS OF ANY MOBILE NUMBER, EMAIL ID, IP ADDRESS IN THE WORLD (STEP BY STEP)



CONVERT ANY MALICIOUS IP INTO URL TO HACK YOUR FRIEND

SEND FAKE MAIL TO HACK YOUR FRIENDS

TOP 6 HACKING MOBILE APPS – MUST HAVE

HACK WHATSAPP ACCOUNT OF YOUR FRIEND

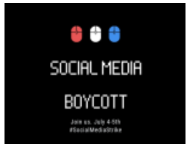
VIEW ALL

MALWARE

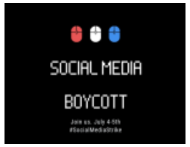
GRANDCRAB RANSOMWARE MASTER KEYS RELEASED BY THE FBI

HACKERS ENCRYPT ALL COLLEGE COMPUTERS WITH RANSOMWARE: $2 MILLION RANSOM

MORE THAN 25 MILLION SMARTPHONES INFECTED WITH NEW MALWARE HIDDEN IN WHATSAPP



NEW RANSOMWARE INFECTS WINDOWS MACHINES EVEN WITHOUT CLICKING OR OPENING AN EMAIL

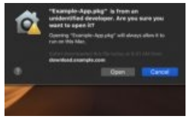


HACKERS EARN MILLIONS WITH THIS ATM CASHOUT MALWARE

HOW DO YOU CHECK THAT A WEBSITE IS UNSAFE?

FACEBOOK PAGES INFECTING THOUSANDS OF USER WITH VIRUS

YOU CAN HACK BANKS WITH THIS MICROSOFT EXCEL ATTACK



“Example-App.pkg” is from an unidentified developer. Are you sure you want to open it?

Opening “Example-App.pkg” will always allow it to run on this Mac.

[illegible]
download.example.com

NEW VULNERABILITY ON MAC IS EXPLOITED WITH MALWARE

PLUROX, THE ALL-IN-ONE MALWARE INFECTING COMPUTERS AROUND THE WORLD

NEW TOOL TO REMOVE GANDCRAB RANSOMWARE ENCRYPTION

YOUR IOT DEVICES, SUCH AS CAMERAS, WASHING MACHINES, NAS STORAGE WILL BE AFFECTED BY THIS NEW MALWARE

CYBERATTACKS AGAINST GAMER COMMUNITY KEEP GROWING

COMPANIES WITH ORACLE WEBLOGIC MUST BE CAREFUL; CRYPTOMINING MALWARE AFFECTS SERVERS

FIRST IT WAS BALTIMORE, NOW PHILADELPHIA IS UNDER MALWARE ATTACK

TWENTY YEARS IN PRISON FOR HACKERS/FOUNDERS OF MARIPOSA BOTNET AND BITCOIN PLATFORM NICEHASH

A HACKER TRICK GOOGLE TO INSTALL A BACKDOOR ON ANDROID PHONES AROUND THE WORLD; HOW DID HE DO IT?

≡

VIEW ALL

CYBER SECURITY CHANNEL

POPULAR NEWS VIDEO 11 JULY

POPULAR NEWS VIDEO 10 JULY

POPULAR NEWS VIDEO 9 JULY

HOW DO YOU CHECK THAT A WEBSITE IS UNSAFE?

CREATE WINDOWS 10 FUD (FULLY UNDETECTABLE) PAYLOAD

TOP 5 TOOLS USED BY CYBER CRIMINALS RECENTLY

How to hack WhatsA...
There is an app which allows to Hack upto 10 WhatsApp Account
3:39 PM
WHATSAPP

HACK WHATSAPP ACCOUNT OF YOUR FRIEND

WIPRO IS HACKED!

CONTACT US

✉ f 🐦 ▶ G