Welcome to
Cyber Security Training

Footprinting Concepts

Objectives of Footprinting

The major objectives of Footprinting are:

1. To know security posture
2. To reduce focus area
3. Identify vulnerabilities
4. Draw network map

Footprinting Methodology

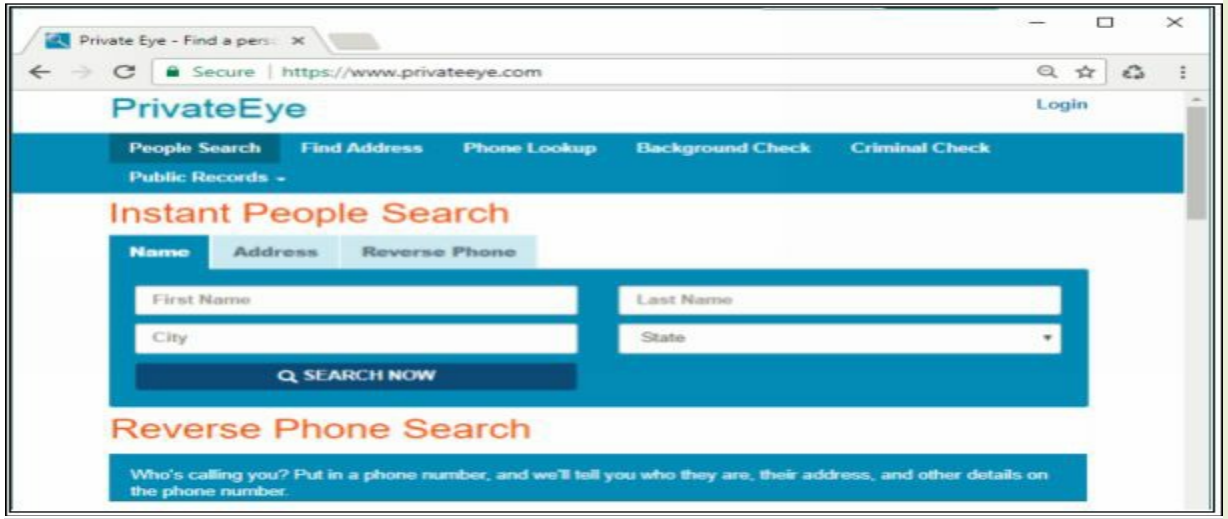
- Footprinting through Search Engines
- Footprinting through Advance Google Hacking Techniques
- Footprinting through Social Networking Sites
- Footprinting through Websites
- Footprinting through Email
- Footprinting through Competitive Intelligence
- Footprinting through WHOIS
- Footprinting through DNS
- Footprinting through Network
- Footprinting through Social Engineering

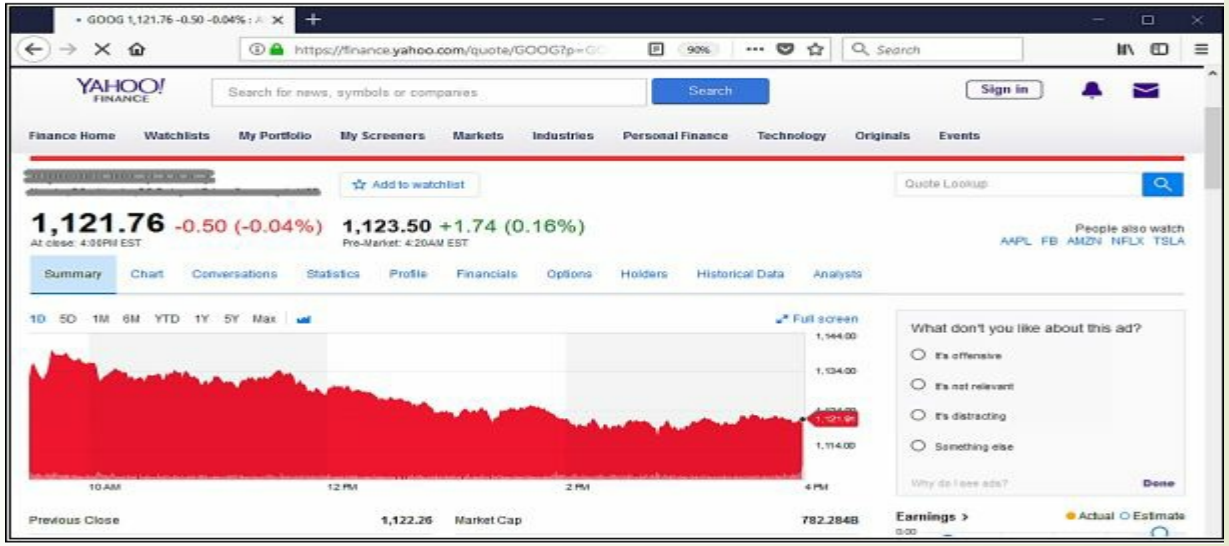
People Search Online Services

There are some online services, popularly used to identify the Phones numbers, Addresses, and People.
Some of these websites include:
www.privateeye.com
www.publicbackgroundchecks.com
www.anywho.com
www.intelius.com
www.4111.com
www.peoplefinders.com

Gather Information from Financial Services:
www.google.com/finance
finance.yahoo.com

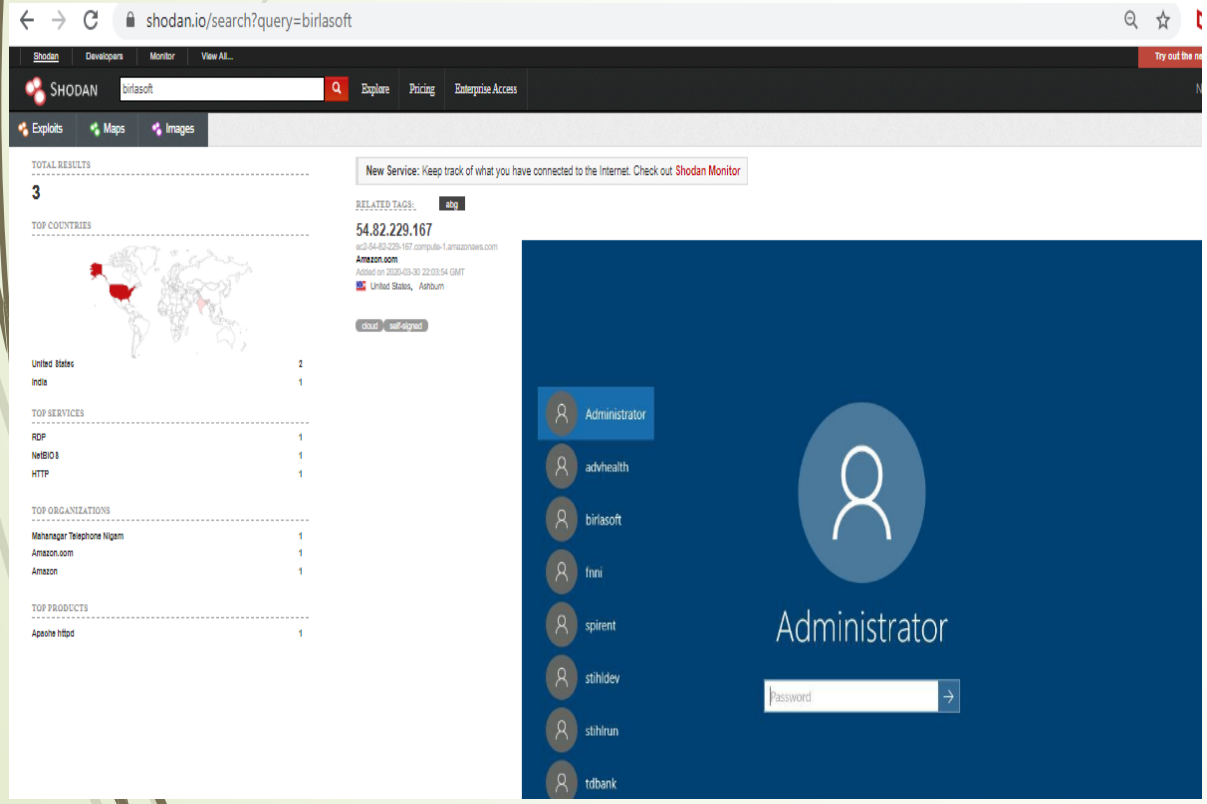
Footprinting using Advanced Google Hacking Techniques

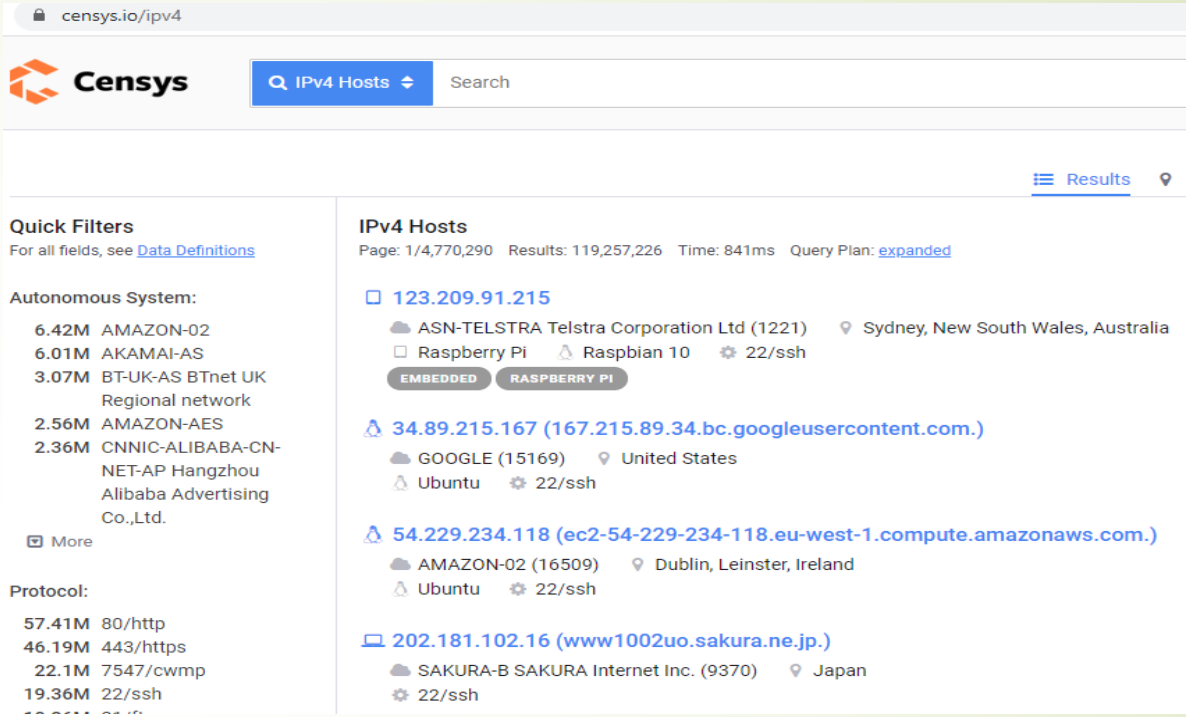


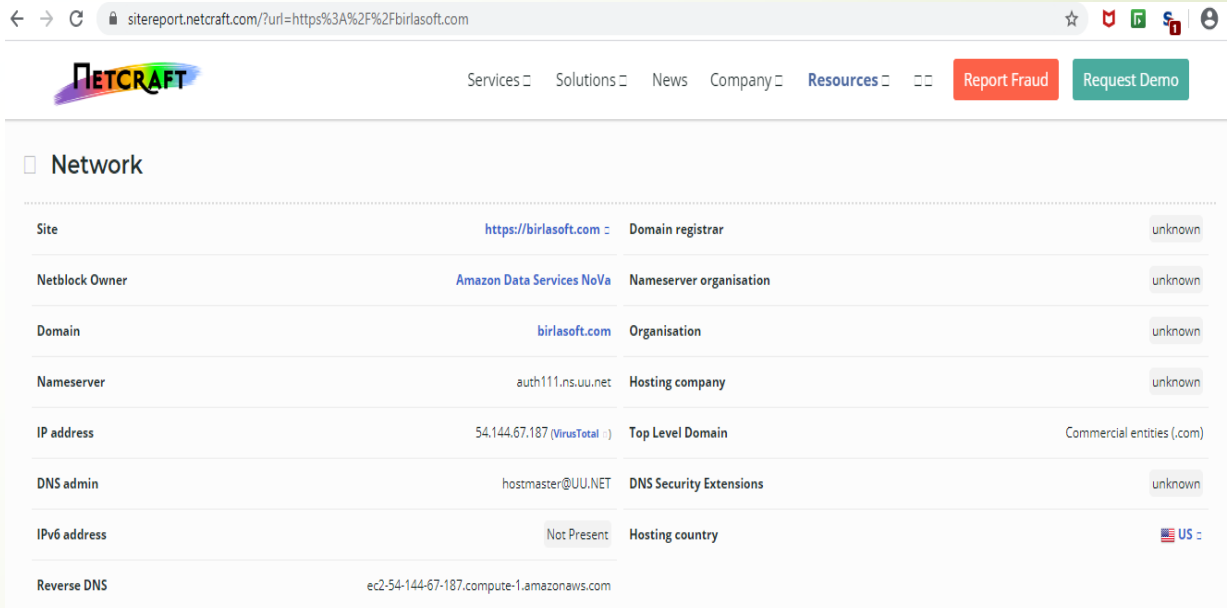


Website Footprinting

netcraft.com
Shodan.io
censys.io



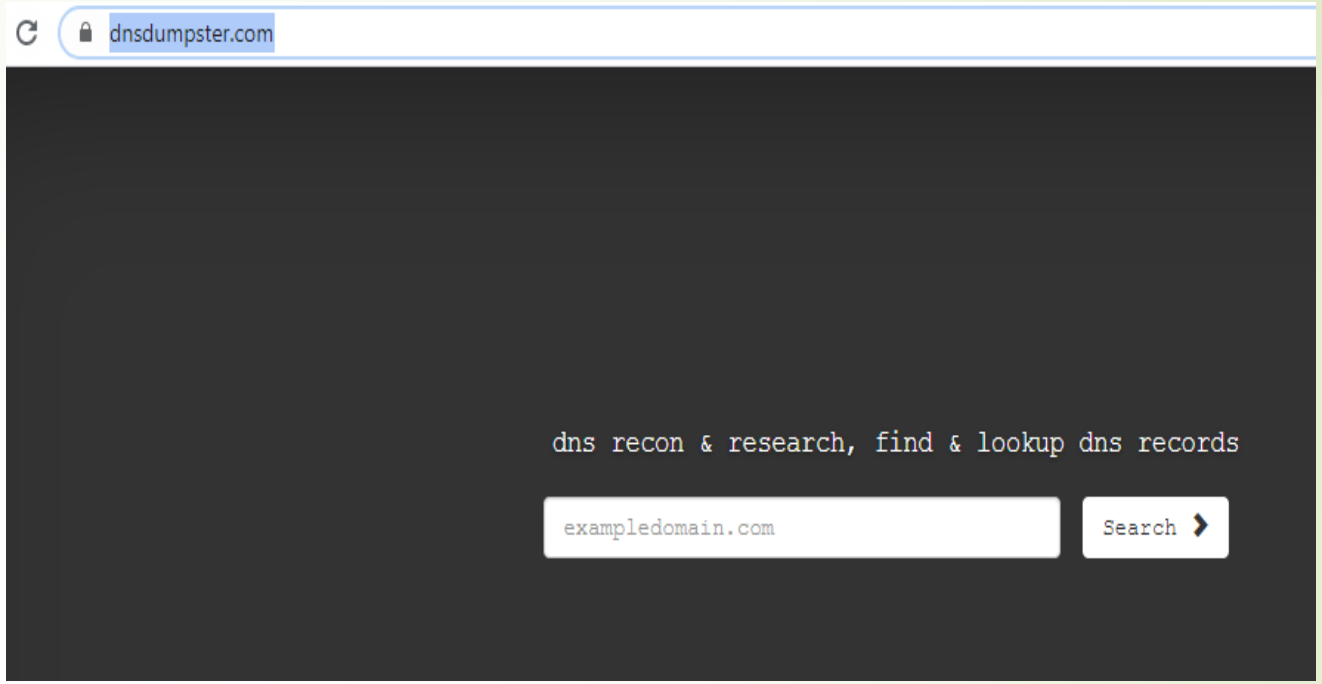


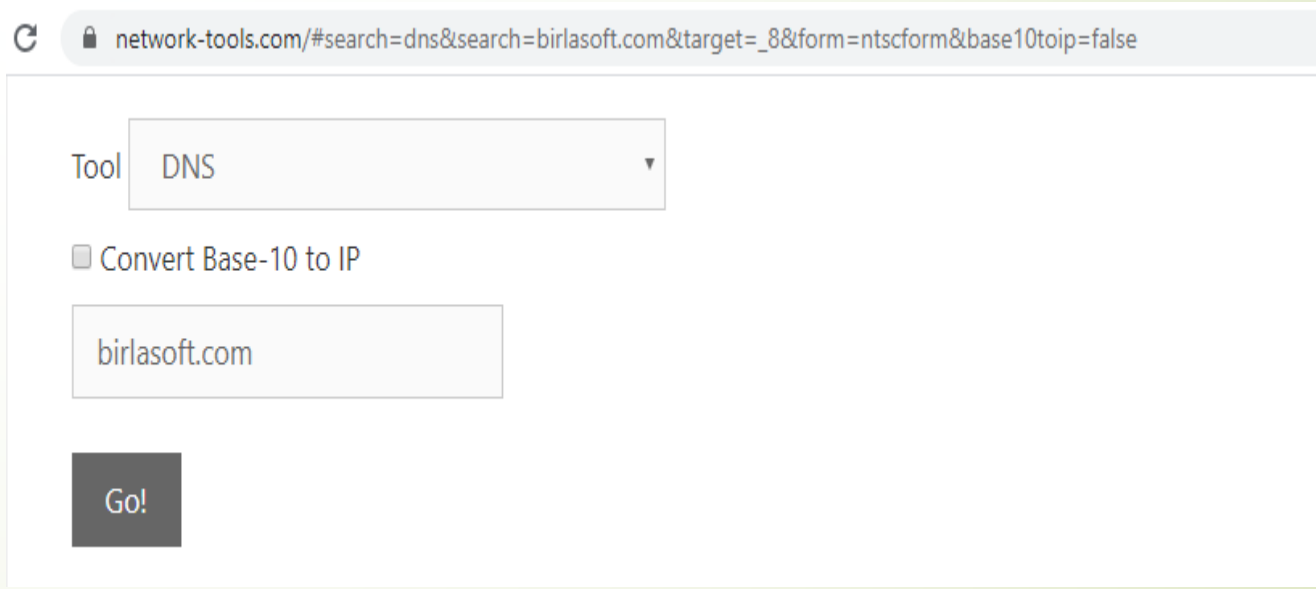


DNS Footprinting

There are a lot of online tools available for DNS lookup information, some of them are listed below:

https://dnsdumpster.com/
http://network-tools.com
http://www.kloth.net
http://www.mydnstools.info
http://www.nirsoft.net
http://www.dnswatch.info
http://www.domaintools.com
http://www.dnsqueries.com
http://www.ultratools.com
http://www.webmaster-toolkit.com





Sub Domain Enumeration

Knock.py

Knock.py website.com

```
root@kali:~/knock/knockpy# python knockpy.py target.com
```

```
 _  __                  _
| |/ /                 | |   4.1.1
| ' / _ __   ___   ___ | | ___ __  _   _
|  < | '_ \ / _ \ / __| |/ / '_ \| | | |
| . \| | | | (_) | (__|   <| |_) | |_| |
|_|\_\_| |_|\___/ \___|_|\_\ .__/ \__, |
                           | |     __/ |
                           |_|    |___/

+ checking for virustotal subdomains: SKIP
        VirusTotal API_KEY not found
+ checking for wildcard: NO
+ checking for zonetransfer: NO
+ resolving target: YES
- scanning for subdomain...

Ip Address      Status  Type    Domain Name                 Server
----------      ------  ----    -----------                 ------
130.211.24.197  404     host    ads.target.com
98.129.229.242  200     host    affiliate.target.com        Apache/2.4
66.171.199.41   302     alias   affiliates.target.com
66.171.199.41   302     host    aff_target.irwhitelabel.com
```

```
 _  __                  _
| |/ /                 | |   4.1
| ' / _ __   ___   ___ | | ___ __  _   _
|  < | '_ \ / _ \ / __| |/ / '_ \| | | |
| . \| | | | (_) | (__|   <| |_) | |_| |
|_|\_\_| |_|\___/ \___|_|\_\ .__/ \__, |
                           | |     __/ |
                           |_|    |___/

- checking for virustotal subdomains: YES

   "a.ns.hackerone.com",
   "b.ns.hackerone.com",
   "api.hackerone.com",
   "links.hackerone.com",
   "support.hackerone.com",
   "info.hackerone.com",
   "www.hackerone.com"

- checking for wildcard: NO
- checking for zonetransfer: NO
- resolving target: YES
- scaning for subdomain...

Ip Address      Status  Type    Domain Name                 Server
----------      ------  ----    -----------                 ------
162.159.0.31            host    a.ns.hackerone.com
104.16.99.52    301     host    api.hackerone.com           cloudflare-nginx
104.16.100.52   301     host    api.hackerone.com           cloudflare-nginx
162.159.1.31            host    b.ns.hackerone.com
104.16.12.26    301     host    support.hackerone.com       cloudflare-nginx
104.16.13.26    301     host    support.hackerone.com       cloudflare-nginx
104.16.99.52    301     host    www.hackerone.com           cloudflare-nginx
104.16.100.52   301     host    www.hackerone.com           cloudflare-nginx
```

Sub Domain Enumeration - Dnsenum

```
root@kali:~# dnsenum --enum google.com
dnsenum.pl VERSION:1.2.3
Host's addresses:
__________________

google.com.                              62       IN    A        74.125.130.100
google.com.                              62       IN    A        74.125.130.101
google.com.                              62       IN    A        74.125.130.102
google.com.                              62       IN    A        74.125.130.113
google.com.                              62       IN    A        74.125.130.138
google.com.                              62       IN    A        74.125.130.139


Name Servers:
_____________

ns1.google.com.                          343227   IN    A        216.239.32.10
ns2.google.com.                          343227   IN    A        216.239.34.10
ns3.google.com.                          343227   IN    A        216.239.36.10
ns4.google.com.                          343227   IN    A        216.239.38.10


Mail (MX) Servers:
__________________

aspmx.l.google.com.                      17       IN    A        74.125.129.27
alt1.aspmx.l.google.com.                 38       IN    A        74.125.142.26
alt3.aspmx.l.google.com.                 178      IN    A        173.194.68.27
alt4.aspmx.l.google.com.                 163      IN    A        74.125.131.27
alt2.aspmx.l.google.com.                 293      IN    A        74.125.137.27
```

Sub Domain Enumeration - Dmitry

Dmitry –wnspb target.com

```
root@kali:~# dmitry -w facebook.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:31.13.79.35
HostName:facebook.com

Gathered Inic-whois information for facebook.com
---------------------------------
   Domain Name: FACEBOOK.COM
   Registry Domain ID: 2320948_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.registrarsafe.com
   Registrar URL: http://www.registrarsafe.com
   Updated Date: 2019-10-17T18:52:06Z
   Creation Date: 1997-03-29T05:00:00Z
   Registry Expiry Date: 2028-03-30T04:00:00Z
   Registrar: RegistrarSafe, LLC
   Registrar IANA ID: 3237
   Registrar Abuse Contact Email: abusecomplaints@registrarsafe.com
   Registrar Abuse Contact Phone: +1-650-308-7004
us: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibit
ed
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibit
```