Reconnaissance and Footprinting

Footprinting

Footprinting is a part of reconnaissance process which is used for gathering possible information about a target computer system or network.

When used in the computer security lexicon, "Footprinting" generally refers to one of the pre-attack phases; tasks performed before doing the actual attack. **Some of the tools used for Footprinting are Sam Spade, nslookup, traceroute, Nmap and neotrace.**

Footprinting Types: Active and Passive

- **Active** - requires attacker to touch the device or network
  - Social engineering and other communication that requires interaction with target
- **Passive** - measures to collect information from publicly available sources
  - Websites, DNS records, business information databases

Footprinting helps to:

- **Know Security Posture** – The data gathered will help us to get an overview of the security posture of the company such as details about the presence of a firewall, security configurations of applications etc.

- **Reduce Attack Area** – Can identify a specific range of systems and concentrate on particular targets only. This will greatly reduce the number of systems we are focussing on.

- **Identify vulnerabilities** – we can build an information database containing the vulnerabilities, threats, loopholes available in the system of the target organization.

- **Draw Network map** – helps to draw a network map of the networks in the target organization covering topology, trusted routers, presence of server and other information.

Footprinting could be both **passive** and **active**. Reviewing a company's website is an example of passive footprinting, whereas attempting to gain access to sensitive information through social engineering is an example of active information gathering.

During this phase, a hacker can collect the following information (only high-level information):

- **Domain name**

- **IP Addresses**
- **Namespaces**
- **Employee information**
- **Phone numbers**
- **E-mails**
- **Job Information**

Can be:

- **Anonymous** - information gathering without revealing anything about yourself
- **Pseudonymous** - making someone else take the blame for your actions

Competitive Intelligence - information gathered by businesses about competitors

Alexa.com - resource for statistics about websites

Footprinting Objectives

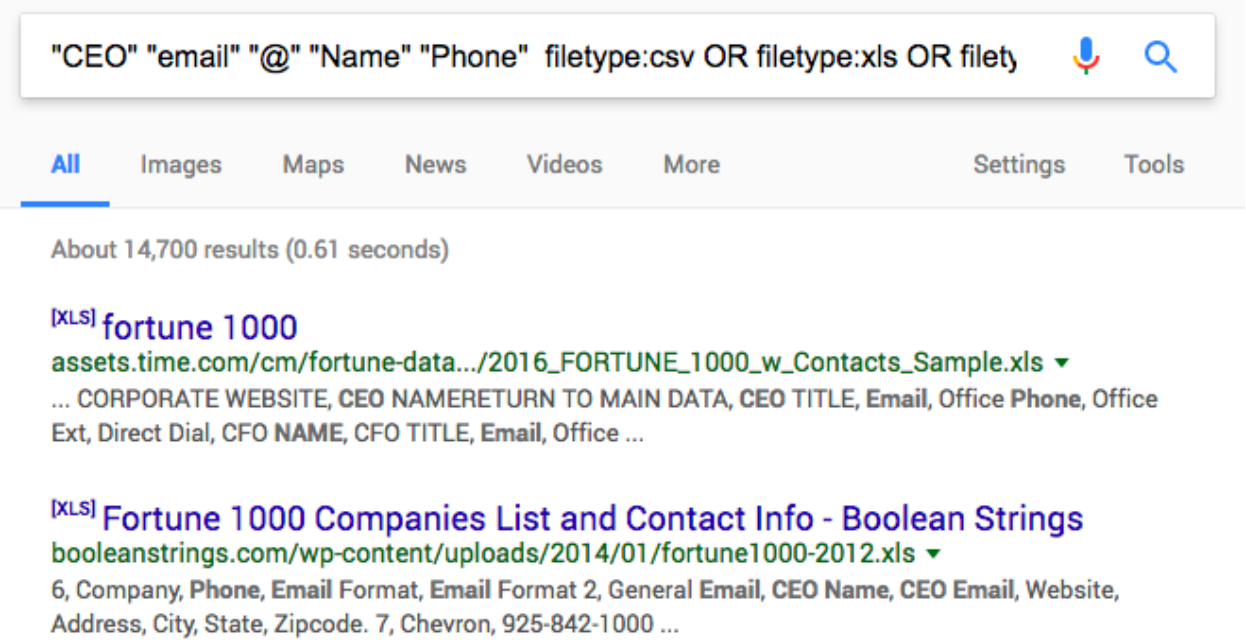
- **Network**
  - DNS
  - IP networks
  - Acessible Systems
  - Websites
  - Access Control
  - VPN Endpoints
  - Firewall vendors
  - IDS Systems
  - Routing/Routed Protocols
  - Phone System (Analog/VoIP)
- **Organization**
  - Org Structure
  - Websites
  - Phone Numbers
  - Directory Information
  - Office Locations
  - Company History
  - Business Associations

- **Hosts**
  - Listening Services
  - Operating System Versions
  - Internet Reachability
  - Enumerated Information
  - SNMP Info
  - Users/Groups
  - Mobile Devices

Methods and Tools

Search Engines

- **NetCraft** - Blueprint a comprehensive list of information about the technologies and information about target website.
  - netcraft
- **Job Search Sites** - Information about technologies can be gleaned from job postings.
- **Google search | Google dorks:**
  - `filetype:` - looks for file types
  - `index of` - directory listings
  - `info:` - contains Google's information about the page
  - `intitle:` - string in title
  - `inurl:` - string in url
  - `link:` - finds linked pages
  - `related:` - finds similar pages
  - `site:` - finds pages specific to that site
    - **Example**:



- GHDB is very good for learn Google Dorks and how it's done in real world scenario

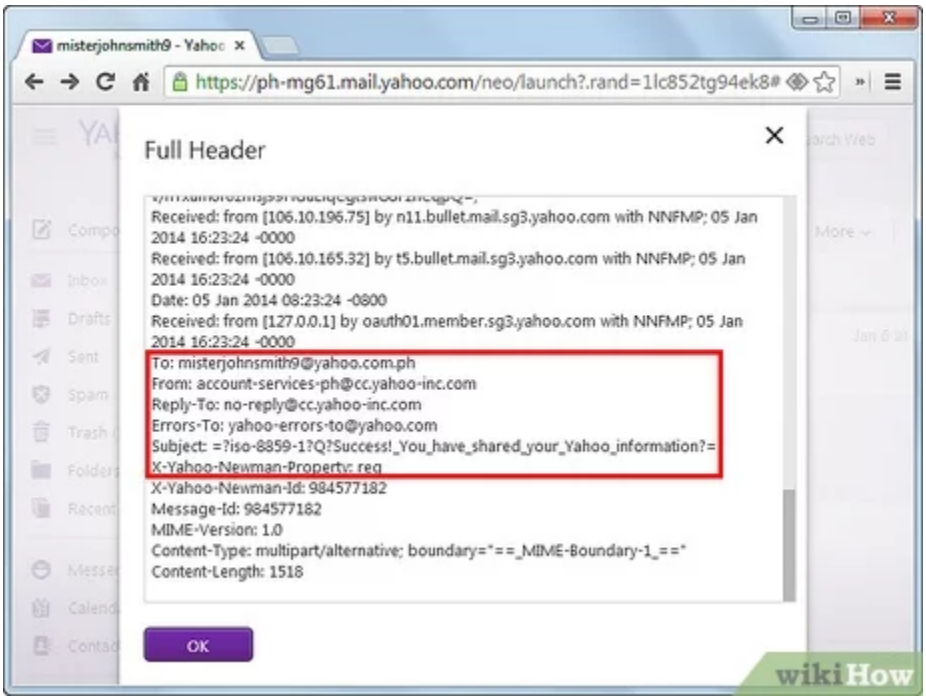
- **Metagoofil** - Command line interface that uses **Google hacks** to find information in meta tags (domain, filetype, etc; Is a google dorks for terminal).

Website Footprinting

- **Web mirroring | Website Cloning** - allows for discrete testing offline
  - **HTTrack** - *you can use the CLI version or Web Interface version*
  - **Wget** - Linux command
    - `wget -mk -w 10 http://hackthissite.org/`
  - **Black Widow**
  - **WebRipper**
  - **Teleport Pro**
  - **Backstreet Browser**
- **Archive.org / Wayback machine**
- Provides cached websites from various dates which possibly have sensitive information that has been now removed.
  - **Wayback Machine -> Google.com**:

- 

Email Footprinting

- **Email header** - may show servers and where the location of those servers are
  - Email headers can provide: **Names, Addresses (IP, email), Mail servers, Time stamps, Authentication and so on.**
    - 

  - **EmailTrackerPro** is a Windows software that trace an email back to its true point of origin:
    - emailtrackerpro
- **Email tracking** - services can track various bits of information including the IP address of where it was opened, where it went, etc.

DNS Footprinting

- Ports
  - Name lookup - UDP 53
  - Zone transfer - TCP 53

- Zone transfer replicates all records
- **Name resolvers** answer requests
- **Authoritative Servers** hold all records for a namespace
- **DNS Record Types**
  -

Name	Description	Purpose
SRV	Service	Points to a specific service
SOA	Start of Authority	Indicates the authoritative NS for a namespace
PTR	Pointer	Maps an IP to a hostname
NS	Nameserver	Lists the nameservers for a namespace
MX	Mail Exchange	Lists email servers
CNAME	Canonical Name	Maps a name to an A reccord
A	Address	Maps an hostname to an IP address

- **DNS Poisoning** - changes cache on a machine to redirect requests to a malicious server
- **DNSSEC** - helps prevent DNS poisoning by encrypting records
- **SOA Record Fields**
  - **Source Host** - hostname of the primary DNS
  - **Contact Email** - email for the person responsible for the zone file
  - **Serial Number** - revision number that increments with each change
  - **Refresh Time** - time in which an update should occur
  - **Retry Time** - time that a NS should wait on a failure
  - **Expire Time** - time in which a zone transfer is allowed to complete
  - **TTL** - minimum TTL for records within the zone
- **IP Address Management**
  - **ARIN** - North America
  - **APNIC** - Asia Pacific
  - **RIPE** - Europe, Middle East
  - **LACNIC** - Latin America
  - **AfriNIC** - Africa
- **Whois** - obtains registration information for the domain from command line or web interface.

- on Kali, whois is pre-installed on CLI; e.g: `whois google.com`)
- on Windows, you can use **SmartWhois** GUI software to perform a whois, or any website like domaintools.com

- **Nslookup** - Performs DNS queries; (nslookup is pre-installed on Kali Linux)
  - `nslookup www.hackthissite.org`
  -
    ```
    Server:         192.168.63.2
    Address:        192.168.63.2#53

    Non-authoritative answer:
    Name:   www.hackthissite.org
    Address: 137.74.187.103
    Name:   www.hackthissite.org
    Address: 137.74.187.102
    Name:   www.hackthissite.org
    Address: 137.74.187.100
    Name:   www.hackthissite.org
    Address: 137.74.187.101
    Name:   www.hackthissite.org
    Address: 137.74.187.104
    ```

    - First two lines shows my current DNS server; The IP addresses returned are '**A record**', meaning is the IPv4 address of the domain; Bottom line NsLookup queries the specified DNS server and retrieves the requested records that are associated with the domain.
    - **The following types of DNS records are especially useful to use on Nslookup:**
    -

Type	Description
A	the IPv4 address of the domain
AAAA	the domain's IPv6 address
CNAME	the canonical name — allowing one domain name to map on to another. This allows more than one website to refer to a single web server.
MX	the server that handles email for the domain.
NS	one or more authoritative name server records for the domain.
TXT	a record containing information for use outside the DNS server. The content takes the form name=value. This information is used for many things including authentication schemes such as SPF and DKIM.

- **Nslookup - Interactive mode zone transfer** (Interactive mode allows the user to query name servers for information about various hosts and domains or to print a list of hosts in a domain).
  - `nslookup`
  - `server <IP Address>`
  - `set type = <DNS type>`
  - `<target domain>`
-
```
nslookup
> set type=AAAA
> www.hackthissite.org
Server:         192.168.63.2
Address:        192.168.63.2#53

Non-authoritative answer:
Name:   www.hackthissite.org
Address: 2001:41d0:8:ccd8:137:74:187:103
Name:   www.hackthissite.org
Address: 2001:41d0:8:ccd8:137:74:187:102
Name:   www.hackthissite.org
Address: 2001:41d0:8:ccd8:137:74:187:101
Name:   www.hackthissite.org
Address: 2001:41d0:8:ccd8:137:74:187:100
Name:   www.hackthissite.org
Address: 2001:41d0:8:ccd8:137:74:187:104
```

- **Dig** - unix-based command like nslookup
  - `dig <target>`
  -
```
dig www.hackthissite.org

; <<>> DiG 9.16.2-Debian <<>> www.hackthissite.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51391
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
;; QUESTION SECTION:
;www.hackthissite.org.          IN      A

;; ANSWER SECTION:
www.hackthissite.org.   5       IN      A       137.74.187.104
```

```
www.hackthissite.org.   5       IN      A       137.74.187.101
www.hackthissite.org.   5       IN      A       137.74.187.100
www.hackthissite.org.   5       IN      A       137.74.187.102
www.hackthissite.org.   5       IN      A       137.74.187.103

;; Query time: 11 msec
;; SERVER: 192.168.63.2#53(192.168.63.2)
;; WHEN: Tue Aug 11 15:05:01 EDT 2020
;; MSG SIZE  rcvd: 129
```

- To get email records specify `-t MX`
  - `dig <target> -t MX`
- To get zone transfer specify `axfr`

Network Footprinting

- IP address range can be obtained from regional registrar (e.g: ARIN for America, RIPE for Europe, etc)
- Use `traceroute` to find intermediary servers
  - traceroute uses ICMP echo in Windows (tracert)
  - traceroute is good for detect Firewalls and the network path

Usage example:

- **`traceroute -I nsa.gov`**
  - Specify target: `traceroute <target>`
  - In this case is used ICMP ECHO for tracerouting: `-I`

```
traceroute -I nsa.gov
traceroute to nsa.gov (104.83.73.99), 30 hops max, 60 byte packets
 1  192.168.63.2 (192.168.63.2)  0.194 ms  0.163 ms  0.150 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  a104-83-73-99.deploy.static.akamaitechnologies.com (104.83.73.99)  42.742 ms  42.666 ms
```

```
25.176 ms
```

> ⚠️ Windows command - `tracert` ⚠️ Linux Command - `traceroute`

Other Relevant Tools

OSRFramework

> ⚡ OSRFramework has a practical lab

Uses open source intelligence to get information about target. *(Username checking, DNS lookups, information leaks research, deep web search, regular expressions extraction, and many others)*.

Web Spiders

Obtain information from the website such as pages, etc.

Recon-ng

> ⚡ Recon-ng has a practical lab

Recon-ng is a web-based open-source reconnaissance tool used to extract information from a target organization and its personnel.

Provides a powerful environment in which open source web-based reconnaissance can be automated conducted, quickly and thoroughly.

Metasploit Framework

> ⚡ Metasploit has a practical lab

The Metasploit Framework is a tool that provides information about security vulnerabilities and aids in penetration testing and IDS signature development; **This is a huge framework that provide Recon tools as well.**

theHarvester

> ⚡ theHarvester has a practical lab

theHarvester is a OSINT tool; Useful for gathering information like:

- Emails
- Subdomains

- Hosts
- Employee names
- Open ports
- Banners from different public sources like search engines, PGP key servers and SHODAN computer database.

Usage example:

- `theHarvester -d www.hackthissite.org -n -b  google`
  - Issue theHarvester command: `theHarvester`
  - Specify the domain: `-d <url>`
  - Perform dns lookup: `-n`
  - Specify search engine/source: `-b google`

```
theHarvester -d www.hackthissite.org -n -b  google
table results already exists

*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 3.1.0                                          *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


[*] Target: www.hackthissite.org

[*] Searching Google.
        Searching 0 results.
        Searching 100 results.
        Searching 200 results.
        Searching 300 results.
        Searching 400 results.
        Searching 500 results.

[*] No IPs found.

[*] Emails found: 2
----------------------
ab790c1315@www.hackthissite.org
```

```
staff@hackthissite.org

[*] Hosts found: 7
---------------------
0.loadbalancer.www.hackthissite.org:
22www.hackthissite.org:
2522www.hackthissite.org:
253dwww.hackthissite.org:
www.hackthissite.org:137.74.187.104, 137.74.187.100, 137.74.187.101, 137.74.187.103,
137.74.187.102
x22www.hackthissite.org:

[*] Starting active queries.
137.74.187.100
[*] Performing reverse lookup in 137.74.187.0/24
module 'theHarvester.discovery.dnssearch' has no attribute 'DnsReverse'
```

Sublist3r

Sublist3r **enumerates subdomains** using many search engines such as Google, Yahoo, Bing, Baidu and Ask. Sublist3r also enumerates subdomains using Netcraft, Virustotal, ThreatCrowd, DNSdumpster and ReverseDNS

Usage example:

- `python3 sublist3r.py -d hackthissite.org`
  - Specify the domain: `-d <url>`

```
python3 sublist3r.py -d hackthissite.org


                 ____        _     _ _     _   _____
                / ___| _   _| |__ | (_)___| |_|___ / _ __
                \___ \| | | | '_ \| | / __| __| |_ \| '__|
                 ___) | |_| | |_) | | \__ \ |_ ___) | |
                |____/ \__,_|_.__/|_|_|___/\__|____/|_|

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for hackthissite.org
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
```

```
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[-] Total Unique Subdomains Found: 41
www.hackthissite.org
admin.hackthissite.org
api.hackthissite.org
ctf.hackthissite.org
vm-005.outbound.firewall.hackthissite.org
vm-050.outbound.firewall.hackthissite.org
vm-099.outbound.firewall.hackthissite.org
vm-150.outbound.firewall.hackthissite.org
vm-200.outbound.firewall.hackthissite.org
forum.hackthissite.org
forums.hackthissite.org
git.hackthissite.org
irc.hackthissite.org
(...)
```

DIRB

DIRB is a Web Content Scanner. It looks for existing (and/or hidden) Web Objects. It basically works by launching a dictionary based attack/brute force attack against a web server and analyzing the response.

- Useful to find subdirectories on web application

Usage example:

- **`dirb https://www.hackthissite.org/ /usr/share/wordlists/dirb/small.txt`**
  - Specify the url by issuing dirb command: `dib <url>`
  - Specify the wordlist: `/path/to/wordlist`

```
dirb https://www.hackthissite.org/ /usr/share/wordlists/dirb/small.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

URL_BASE: https://www.hackthissite.org/
WORDLIST_FILES: /usr/share/wordlists/dirb/small.txt

-----------------

GENERATED WORDS: 959
```

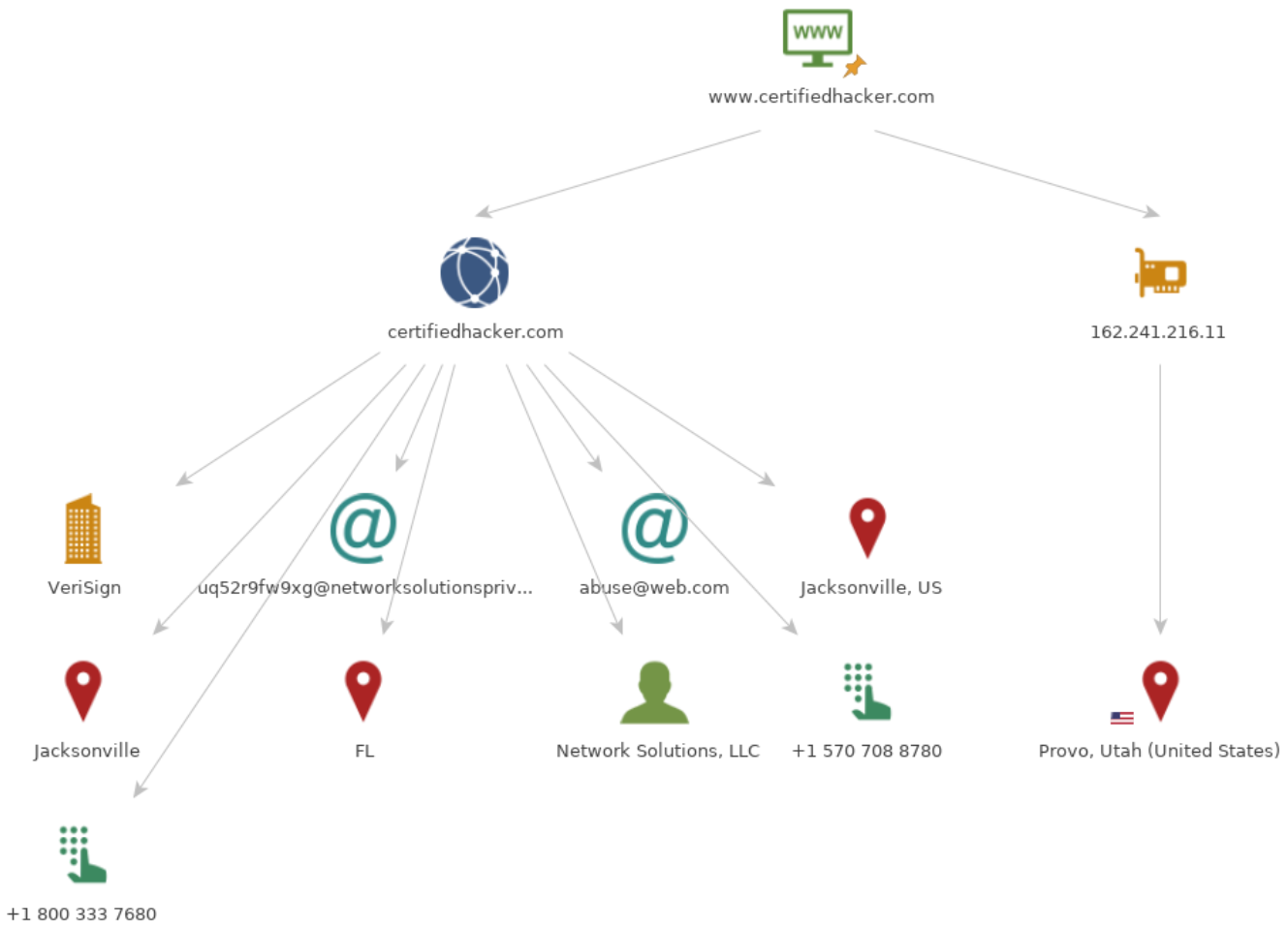
```
---- Scanning URL: https://www.hackthissite.org/ ----
+ https://www.hackthissite.org/api (CODE:200|SIZE:10)
+ https://www.hackthissite.org/blog (CODE:200|SIZE:20981)
+ https://www.hackthissite.org/cgi-bin/ (CODE:403|SIZE:199)
```

Maltego

> ⚡ Maltego has practical labs

Maltego is a powerful OSINT tool, you can extract a broad type of information through the network, technologies and personnel(email, phone number, twitter).

- You able to:
  - Identify IP address
  - Identify Domain and Domain Name Schema
  - Identify Server Side Technology
  - Identify Service Oriented Architecture (SOA) information
  - Identify Name Server
  - Identify Mail Exchanger
  - Identify Geographical Location
  - Identify Entities
  - Discover Email addresses and Phone numbers



Social Engineering Framework (SEF)

It's a open source Social Engineering Framework (SCRIPT) that helps generate phishing attacks and fake emails. and it's includes phishing pages, fake email, fake email with file attachment and other stuff that helps you in Social Engineering Attack.

sef

Web Based Recon

NetCraft

Netcraft is a website analyzing server, with the help of this website we find basic and important information on the website like:

- **Background** — This includes basic domain information.
  - Which OS, Web server is runing; Which ISP;
- **Network** — This includes information from IP Address to Domain names to nameservers.

- **SSL/TLS** — This gives the ssl/tls status of the target
- **Hosting History** - This gives the information on the hosting history of the target
- **Sender Policy Framework (SPF)** — This describes who can send mail on the domains behalf
- **DMARC** -This is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated
- **Web Trackers** — This trackers can be used to monitor individual user behavior across the web
  Site Technology — This section includes details on:
  - Cloud & PaaS
  - Server-Side technologies (e.g: PHP)
  - Client-Side technologies (e.g: JavaScript library)
  - CDN Information
  - CMS Information (e.g: Wordpress, Joomla, etc)
  - Mobile Technologies
  - Web stats (e.g: Web analytics, collection, etc)
  - Character encoding

netcraft

Shodan

Shodan Unlike traditional search engines such as Google, use Web crawlers to traverse your entire site, but directly into the channel behind the Internet, various types of port equipment audits, and never stops looking for the Internet and all associated ***servers, camera, printers, routers, and so on****.*

- Some have also described it as a search engine of service banners, which are metadata that the server sends back to the client.

- Shodan works well with basic, single-term searches. Here are the basic search filters you can use:

  - **city:** find devices in a particular city
  - **country:** find devices in a particular country
  - **geo:** you can pass it coordinates
  - **hostname:** find values that match the hostname
  - **net:** search based on an IP or /x CIDR
  - **os:** search based on an operating system
  - **port:** find particular ports that are open
  - **before/after:** find results within a timeframe

Shodan | Developers | Monitor | View All... | Show API Key | Help Center

SHODAN

port:9200 json

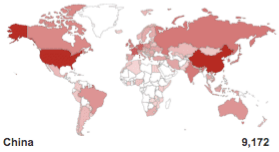
Explore | Downloads | Reports | Pricing | Enterprise Access | My Account | Upgrade

Exploits | Maps | Like 43 | Download Results | Create Report

TOTAL RESULTS

29,183

TOP COUNTRIES



China	9,172
United States	8,202
France	1,657
Germany	1,411
Netherlands	1,154

TOP ORGANIZATIONS

Hangzhou Alibaba Advertising...	4,774
Amazon.com	3,392
Google Cloud	1,713
Microsoft Azure	1,564
Digital Ocean	1,059

TOP OPERATING SYSTEMS

Linux 3.x	7
Windows 7 or 8	3
linux	1
FreeBSD 9.x	1

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

RELATED TAGS: https://www.instagram.com/sxse_18/

52.232.101.70
Microsoft Azure
Added on 2019-05-02 12:43:26 GMT
Netherlands, Amsterdam

cloud

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Basic realm="security" charset="UTF-8"
content-type: application/json; charset=UTF-8
content-length: 369
```

47.111.48.179
Hangzhou Alibaba Advertising Co.,Ltd.
Added on 2019-05-02 12:49:42 GMT
China

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Basic realm="security" charset="UTF-8"
content-type: application/json; charset=UTF-8
content-length: 369
```

138.201.48.14
static.14.48.201.138.clients.your-server.de
Hetzner Online GmbH
Added on 2019-05-02 12:43:58 GMT
Germany, Heidelberg

database

```
HTTP/1.1 200 OK
content-type: application/json; charset=UTF-8
content-length: 433
```

47.101.196.119
Hangzhou Alibaba Advertising Co.,Ltd.
Added on 2019-05-02 12:45:31 GMT
China

20.0 | 1

```
HTTP/1.1 200 OK
content-type: application/json; charset=UTF-8
```

SHODAN

Netgear DGN1000

Exploits | Maps | Share Search

TOTAL RESULTS

4,799

TOP COUNTRIES

Italy	1,156
United Kingdom	982
South Africa	785
United States	245
Kuwait	236

TOP SERVICES

HTTP (8080)	3,598
HTTP	661
Synology	121
8081	107
HTTPS (8443)	23

Censys

Alternative for Shodan.