BUG BOUNTY ASSIGNMENT

Domain	: https://www.airbnb.com/
Student name	: W.M.K.R. Wanasinghe
Student registration number	: IT22298508
Date of submission	:05/11/2023
Batch	:1.2

Contents

Acknowledgment

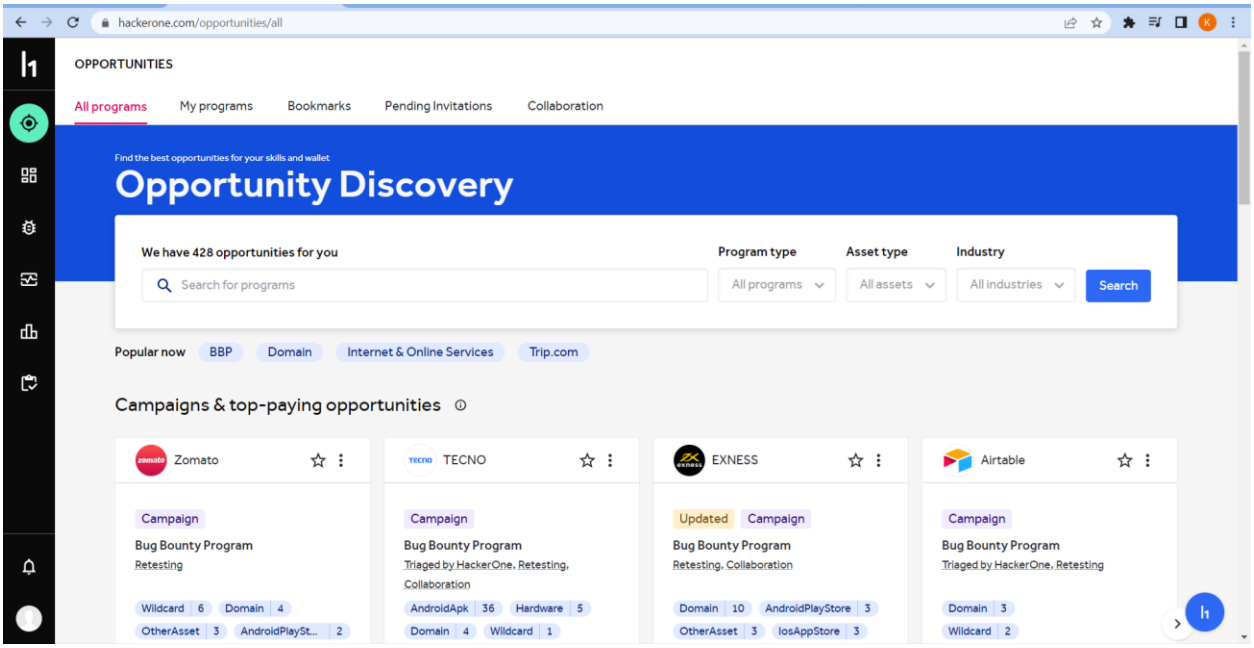
I would like to express my sincere gratitude to Mr warma for his relentless effort in guiding us, advising us through difficult and unfamiliar phases of the project, and helping us gain practical knowledge and skills in the subject.

It is with heartfelt appreciation that I thank mr kohilan for helping me throughout the semester to gain new knowledge and understand concepts of Web security and how to implement them in the practical world.

Purpose

The purpose of this assignment is the assess vulnerabilities of the web application. So, https://www.hackerone.com/ (Fig.1) platform is used to find the websites and web applications for the Bug Bounty hunting. And there are a lot of Bug Bounty hunting platforms to improve our vulnerability assessing skills. As an example, https://www.bugcrowd.com/ is one of the Bug Bounty hunting platforms. So, the purpose of using this HackerOne platform is because this website legally protects us to do Bug Bounty hunting for real-world web applications.

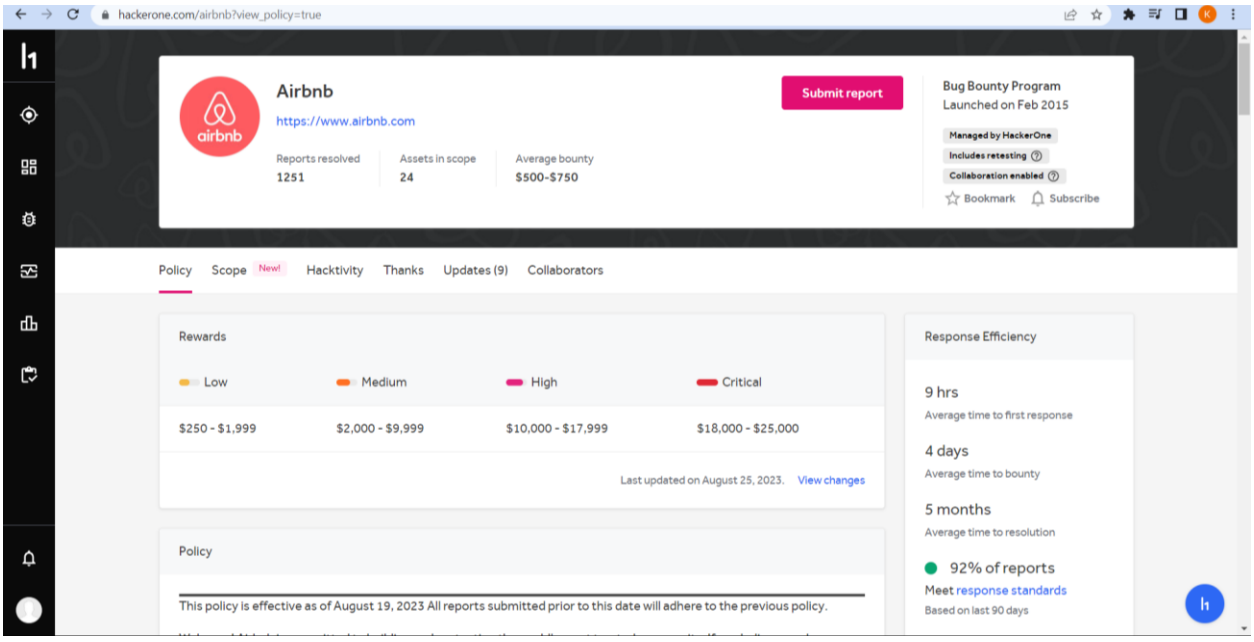
Using these websites benefits to get powerful knowledge about the penetration testing tool and how to use those tools. And these web audit reports are giving an excellent understanding of how to handle cybersecurity profession skills.

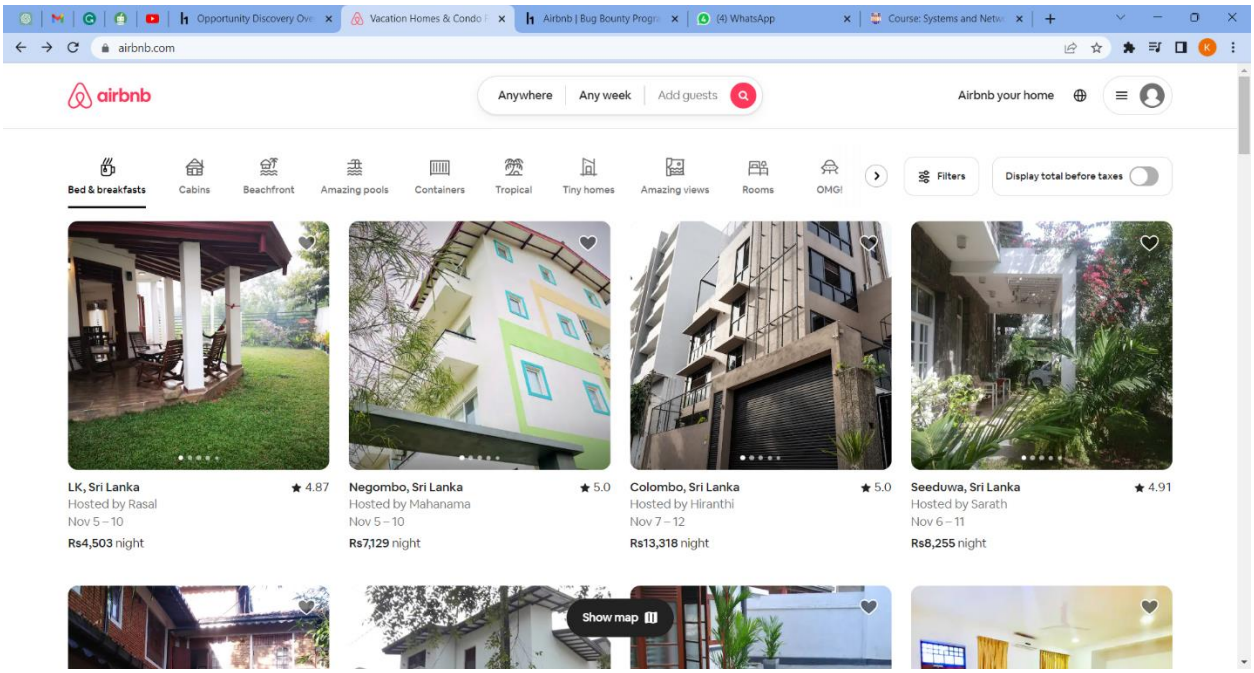


Introduction

Web security is critical to web-based companies and businesses because cybercrime is increasing day by day. Every moment attackers are finding new paths for exploiting the web applications. And attackers develop their skills not only for fun they focus on money also. That is why ransomware attacks are most popular these days. Because of that protection is a must for web applications to defend against this type of cybercrime.

So, a lot of web-based companies and businesses are assigned to Bug Bounty programs to detect the vulnerabilities and fix those vulnerable domains before getting into attack. Hackerone(https://www.hackerone.com/) is one of the platforms that help web-based companies to fix vulnerabilities through Bug Bounty programs. And Hackerone platform and web-based companies are paying for penetration testing their web domains. So, I selected a web-based company called airbnb(https://www.airbnb.com) for my Bug Bounty hunting program. airbnb platform is used by rent houses and rooms for guests.





This Bug Bounty Assignment is used to be done according to the following web application security testing methodology.

- Information gathering
- Planning and analysis
- Vulnerability detection
- Penetration testing
- Reporting

The scope of the investigation was restricted to more than 20 domains of Airbnb.com primary web application.

- support-api.airbnb.com
- omgpro.airbnb.com
- one.airbnb.com
- next.airbnb.com
- hoteltonight.com
- open.airbnb.com

These are the domains selected to perform this Bug Bounty hunting program.

Information gathering

Information gathering is the first step to building a strong foundation for this Bug Bounty hunting program. Because this step is about collecting the critical details of the targeted web application. If this step is not done well entire project can be a useless effort. So, more information means that we can capture more vulnerabilities from targeted domains. As an example, we have to find the targeted domain's IP addresses, details about open ports in the targeted domain, and what type of protection they use to protect their web application. According to the All About Testing (AAT), “The more useful information you have about a target, the more you can find vulnerabilities in the target and find more serious problems in the target by exploiting them.”. So, perfect information gathering is key to unlocking vulnerabilities from the target and it will help improve our vulnerability scanning process.

Information gathering can be divided into two parts. they are,

1. Active information gathering
   - Active information gathering is collecting information from the targeted domain involves monitoring the target systems by building communication with the target. This method is detectable to the targeted system.
2. Passive information gathering
   - Passive information gathering is collecting information from the targeted domain without invoking any kind of communication with the target systems.

Considering the Passive and Active information gathering, there are many tools to gather information from the target domain using both methods. They are,

1. Passive information-gathering tools
   - Sublist3r
   - Nslookup
   - Whois
   - Whatweb
   - Dig
   - Netcraft
   - Whois lookup

2. Active information-gathering tools
    - Nmap
    - Dmitry

These are the information-gathering tools used to analyze the targeted web domain. And I give priority to Passive information-gathering tools. Because Active information gathering is very noisy. But we need active information gathering to analyze information about what is open ports are in our targeted system.

1. Passive information gathering

➢ Sublist3r

Sublist3r is a subdomain enumeration tool. That means this is a tool to identify the unique subdomains associated with the target domain. Because of this tool, we can gather more information about subdomains. This tool is not built-in and comes with Kali Linux operating system and first, we need to install this tool in the Kali Linux operating system.

- Download the sublist3r.

```
┌──(kaveesha㉿kali)-[~]
└─$ git clone https://github.com/aboul3la/Sublist3r.git
fatal: destination path 'Sublist3r' already exists and is not an empty directory.
```

It is already installed.

- Check the downloaded location and go into the sublis3r directory.

```
┌──(kaveesha㉿kali)-[~]
└─$ ls
bash        ex1.c        example1.c          example.c.save.1  'gcc example'          natas.py              recon.sh
Desktop     ex2          example1.c.save     example.c.save.2  'gcc example.c'        Pictures              Sublist3r
Documents   ex2.c        example2.c          example.c.save.3  'gcc example.c.save'   private.key           Templates
Downloads   exa.c        example.c           example.c.save.4   Music                 private.key———BEGIN   Videos
ex          exa.c.save  'example.c gcc ex'   example.save       natas15.py            Public
ex1         example      example.c.save      ex.c.save          natas16.py            recon2.sh
```

```
┌──(kaveesha㉿kali)-[~]
└─$ cd Sublist3r

┌──(kaveesha㉿kali)-[~/Sublist3r]
└─$ ls
LICENSE  MANIFEST.in  README.md  requirements.txt  setup.py  subbrute  sublist3r.py
```

- Install python3-pip in kali Linux.

```
kaveesha@kali: ~
File  Actions  Edit  View  Help
┌──(kaveesha㉿kali)-[~]
└─$ sudo apt install python3-pip
[sudo] password for kaveesha:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
python3-pip is already the newest version (22.3+dfsg-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

- Install dependencies in the sublist3r directory.

```
python3-pip is already the newest version (22.3+dfsg-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

┌──(kaveesha㉿kali)-[~/Sublist3r]
└─$ sudo pip install -r requirements.txt
Collecting argparse
  Using cached argparse-1.4.0-py2.py3-none-any.whl (23 kB)
Requirement already satisfied: dnspython in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2)) (2.2.
1)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requirements.txt (line 3)) (2.27.
1)
Installing collected packages: argparse
Successfully installed argparse-1.4.0
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system p
ackage manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv
```

- Install argparse module in the sublist3r directory.

```
┌──(kaveesha㉿kali)-[~/Sublist3r]
└─$ sudo apt-get install python-argparse
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
Note, selecting 'libpython2.7-stdlib' instead of 'python-argparse'
libpython2.7-stdlib is already the newest version (2.7.18-13.2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

- Check sublist3r is ready to use and test the tool.

```
┌──(kaveesha㉿kali)-[~/Sublist3r]
└─$ ls
LICENSE  MANIFEST.in  README.md  requirements.txt  setup.py  subbrute  sublist3r.py
```

- After installing sublist3r next step is to scan the main domain to capture subdomains in the target system (Airbnb.com).

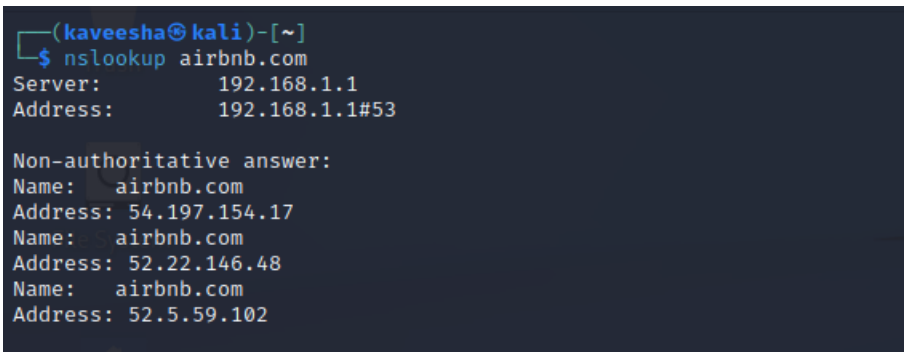
```
┌──(kaveesha㉿kali)-[~/Sublist3r]
└─$ python3 sublist3r.py -d airbnb.com

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

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for airbnb.com
[-] 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..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 160
www.airbnb.com
admin.airbnb.com
prototype.admin.airbnb.com
```

After the scan, the sublist3r tool found 160 unique subdomains related to the main domain (Airbnb.com).

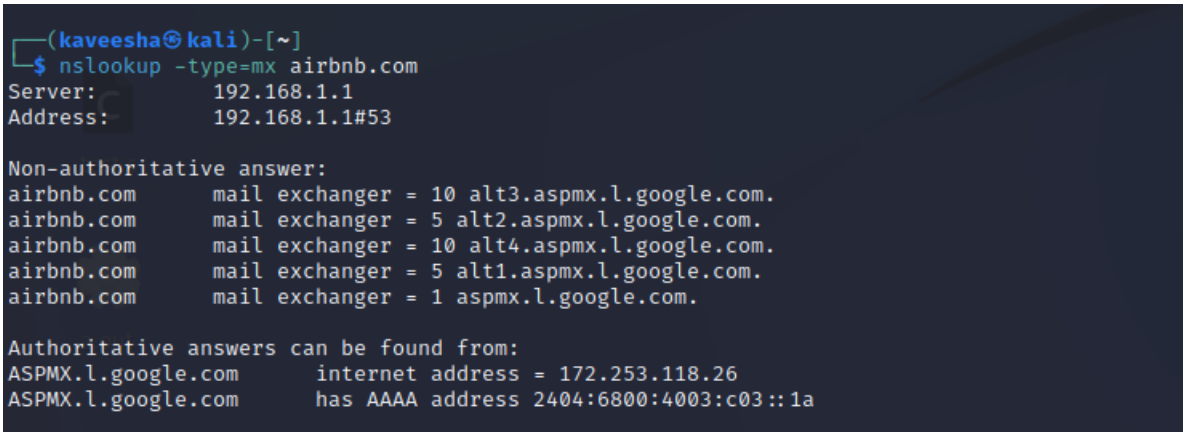
➢ Nslookup

Nslookup is perfect DNS enumeration. That means this is a tool for gathering information about the Domain Name System (DNS) of the targeted system. Nslookup tool help to find out the information related to DNS record names, IP addresses of a target, DNS domain names, and the MX records for the domain or the NS servers of the domain. This tool is already built in the Kali Linux environment. So, I gather the information that. Sublist3r scan results of all selected domains to get a better understanding of DNS information related to the web application (Airbnb.com).

- Gather information about the IP address of the hostname.



- Gather information about the mail exchange (MX) records.



- Gather information about the nameserver (NS) records.

```
┌──(kaveesha㉿kali)-[~]
└─$ nslookup -type=ns airbnb.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
airbnb.com      nameserver = ns-158.awsdns-19.com.
airbnb.com      nameserver = ns-756.awsdns-30.net.
airbnb.com      nameserver = ns-1108.awsdns-10.org.
airbnb.com      nameserver = dns4.p08.nsone.net.
airbnb.com      nameserver = ns-1977.awsdns-55.co.uk.
airbnb.com      nameserver = dns2.p08.nsone.net.
airbnb.com      nameserver = dns3.p08.nsone.net.
airbnb.com      nameserver = dns1.p08.nsone.net.

Authoritative answers can be found from:
dns1.p08.nsone.net      internet address = 198.51.44.8
dns2.p08.nsone.net      internet address = 198.51.45.8
dns3.p08.nsone.net      internet address = 198.51.44.72
dns4.p08.nsone.net      internet address = 198.51.45.72
ns-158.awsdns-19.com    internet address = 205.251.192.158
ns-756.awsdns-30.net    internet address = 205.251.194.244
ns-1108.awsdns-10.org   internet address = 205.251.196.84
ns-1977.awsdns-55.co.uk internet address = 205.251.199.185
dns1.p08.nsone.net      has AAAA address 2620:4d:4000:6259:7:8:0:1
dns2.p08.nsone.net      has AAAA address 2a00:edc0:6259:7:8::2
dns3.p08.nsone.net      has AAAA address 2620:4d:4000:6259:7:8:0:3
dns4.p08.nsone.net      has AAAA address 2a00:edc0:6259:7:8::4
```

- gather information about the “start of authority” (SOA) records. That means we can get details about the domain or region, like the administrator’s email address, how long the server should wait between refreshes, and the very last time the domain was modified.

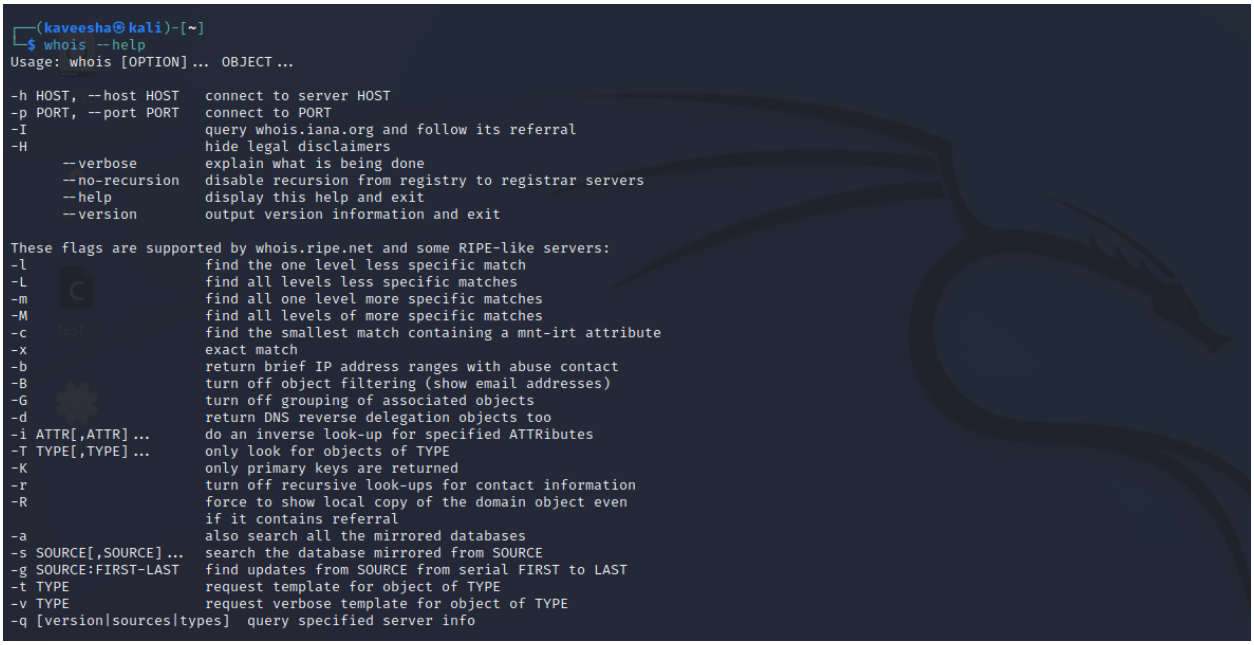
```
┌──(kaveesha㉿kali)-[~]
└─$ nslookup -type=soa airbnb.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
airbnb.com
        origin = ns-1977.awsdns-55.co.uk
        mail addr = awsdns-hostmaster.amazon.com
        serial = 1
        refresh = 7200
        retry = 900
        expire = 1209600
        minimum = 86400

Authoritative answers can be found from:
```

- “ANY” keyword can use gather all the above information using only one command. So, I use that command to gather information on the in-scope domains.

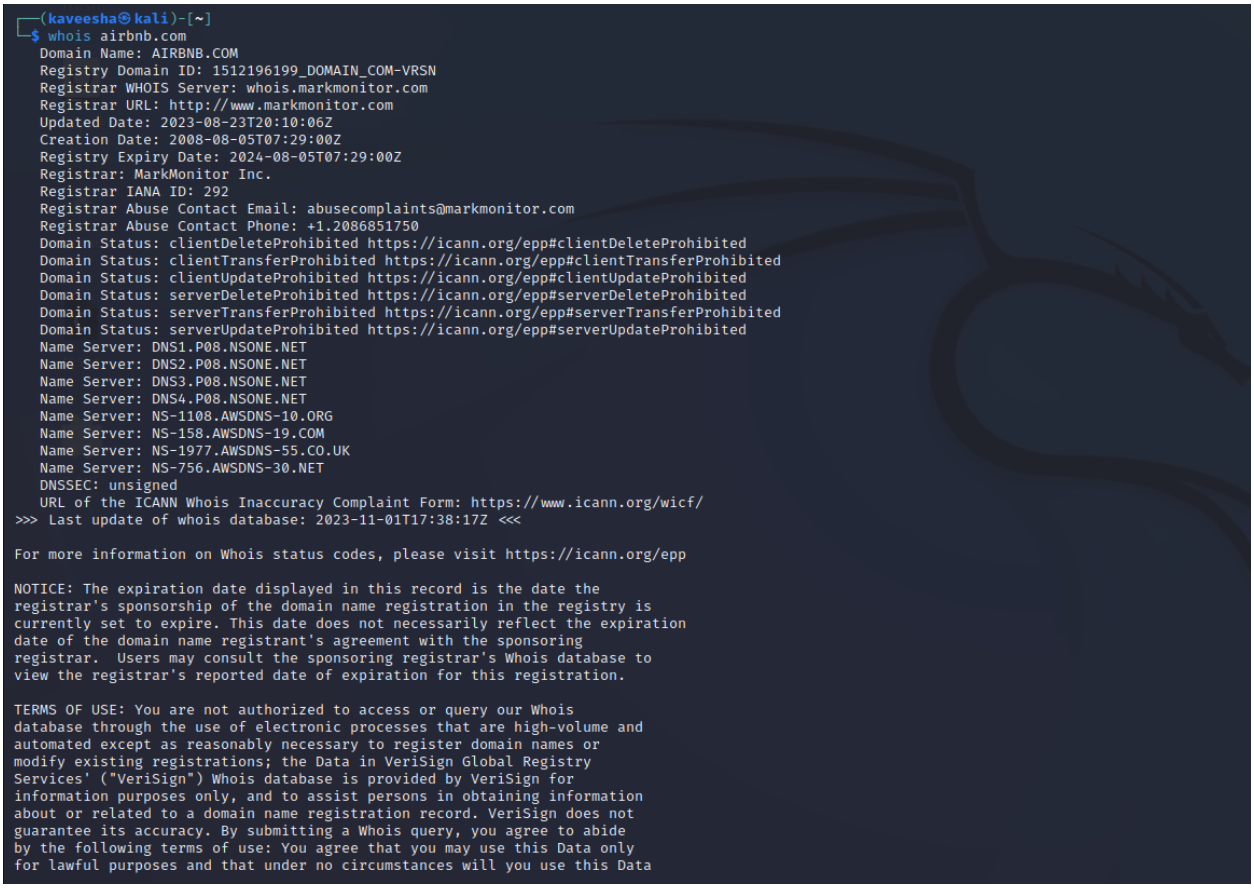
```
┌──(kaveesha㉿kali)-[~]
└─$ nslookup -type=any airbnb.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
airbnb.com      nameserver = ns-1108.awsdns-10.org.
airbnb.com      nameserver = dns3.p08.nsone.net.
airbnb.com      nameserver = ns-158.awsdns-19.com.
airbnb.com      nameserver = dns4.p08.nsone.net.
airbnb.com      nameserver = ns-756.awsdns-30.net.
airbnb.com      nameserver = dns2.p08.nsone.net.
airbnb.com      nameserver = dns1.p08.nsone.net.
airbnb.com      nameserver = ns-1977.awsdns-55.co.uk.

Authoritative answers can be found from:
airbnb.com      nameserver = ns-756.awsdns-30.net.
airbnb.com      nameserver = dns2.p08.nsone.net.
airbnb.com      nameserver = ns-1108.awsdns-10.org.
airbnb.com      nameserver = dns4.p08.nsone.net.
airbnb.com      nameserver = ns-158.awsdns-19.com.
airbnb.com      nameserver = dns1.p08.nsone.net.
airbnb.com      nameserver = ns-1977.awsdns-55.co.uk.
airbnb.com      nameserver = dns3.p08.nsone.net.
dns1.p08.nsone.net      internet address = 198.51.44.8
dns2.p08.nsone.net      internet address = 198.51.45.8
dns3.p08.nsone.net      internet address = 198.51.44.72
dns4.p08.nsone.net      internet address = 198.51.45.72
ns-158.awsdns-19.com    internet address = 205.251.192.158
ns-756.awsdns-30.net    internet address = 205.251.194.244
ns-1108.awsdns-10.org   internet address = 205.251.196.84
ns-1977.awsdns-55.co.uk internet address = 205.251.199.185
dns1.p08.nsone.net      has AAAA address 2620:4d:4000:6259:7:8:0:1
dns2.p08.nsone.net      has AAAA address 2a00:edc0:6259:7:8::2
dns3.p08.nsone.net      has AAAA address 2620:4d:4000:6259:7:8:0:3
dns4.p08.nsone.net      has AAAA address 2a00:edc0:6259:7:8::4
ns-158.awsdns-19.com    has AAAA address 2600:9000:5300:9e00::1
ns-756.awsdns-30.net    has AAAA address 2600:9000:5302:f400::1
ns-1108.awsdns-10.org   has AAAA address 2600:9000:5304:5400::1
ns-1977.awsdns-55.co.uk has AAAA address 2600:9000:5307:b900::1
```

➢ Whois

Whois command gathers information related to targeted domain unknown and distant hosts, server information, network details, and many more details. This command also has a lot of filtering options and uses that “whois --help” command to grant filtering techniques.



I did not want to filter the output because I need a full detailed report for my information gathering process. So, these are the sample output of this command.



```
┌──(kaveesha㉿kali)-[~]
└─$ whois airbnb.com
   Domain Name: AIRBNB.COM
   Registry Domain ID: 1512196199_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2023-08-23T20:10:06Z
   Creation Date: 2008-08-05T07:29:00Z
   Registry Expiry Date: 2024-08-05T07:29:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: DNS1.P08.NSONE.NET
   Name Server: DNS2.P08.NSONE.NET
   Name Server: DNS3.P08.NSONE.NET
   Name Server: DNS4.P08.NSONE.NET
   Name Server: NS-1108.AWSDNS-10.ORG
   Name Server: NS-158.AWSDNS-19.COM
   Name Server: NS-1977.AWSDNS-55.CO.UK
   Name Server: NS-756.AWSDNS-30.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-11-01T17:38:17Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
```

```
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: airbnb.com
Registry Domain ID: 1512196199_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2023-08-23T22:03:11+0000
Creation Date: 2008-08-05T07:29:00+0000
Registrar Registration Expiration Date: 2024-08-05T00:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registrant Organization: Airbnb, Inc.
Registrant State/Province: CA
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/airbnb.com
Admin Organization: Airbnb, Inc.
Admin State/Province: CA
Admin Country: US
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/airbnb.com
Tech Organization: Airbnb, Inc.
Tech State/Province: CA
Tech Country: US
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/airbnb.com
Name Server: ns-158.awsdns-19.com
Name Server: dns3.p08.nsone.net
Name Server: dns4.p08.nsone.net
```

```
Name Server: dns3.p08.nsone.net
Name Server: dns4.p08.nsone.net
Name Server: dns2.p08.nsone.net
Name Server: ns-1108.awsdns-10.org
Name Server: dns1.p08.nsone.net
Name Server: ns-1977.awsdns-55.co.uk
Name Server: ns-756.awsdns-30.net
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2023-11-01T17:38:35+0000 <<<

For more information on WHOIS status codes, please visit:
  https://www.icann.org/resources/pages/epp-status-codes

If you wish to contact this domain's Registrant, Administrative, or Technical
contact, and such email address is not visible above, you may do so via our web
form, pursuant to ICANN's Temporary Specification. To verify that you are not a
robot, please enter your email address to receive a link to a page that
facilitates email communication with the relevant contact(s).

Web-based WHOIS:
  https://domains.markmonitor.com/whois

If you have a legitimate interest in viewing the non-public WHOIS details, send
your request and the reasons for your request to whoisrequest@markmonitor.com
and specify the domain name in the subject line. We will review that request and
may ask for supporting documentation and explanation.

The data in MarkMonitor's WHOIS database is provided for information purposes,
and to assist persons in obtaining information about or related to a domain
name's registration record. While MarkMonitor believes the data to be accurate,
the data is provided "as is" with no guarantee or warranties regarding its
accuracy.

By submitting a WHOIS query, you agree that you will use this data only for
lawful purposes and that, under no circumstances will you use this data to:
  (1) allow, enable, or otherwise support the transmission by email, telephone,
or facsimile of mass, unsolicited, commercial advertising, or spam; or
  (2) enable high volume, automated, or electronic processes that send queries,
data, or email to MarkMonitor (or its systems) or the domain name contacts (or
its systems).

MarkMonitor reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by this policy.

MarkMonitor Domain Management(TM)
Protecting companies and consumers in a digital world.

Visit MarkMonitor at https://www.markmonitor.com
```

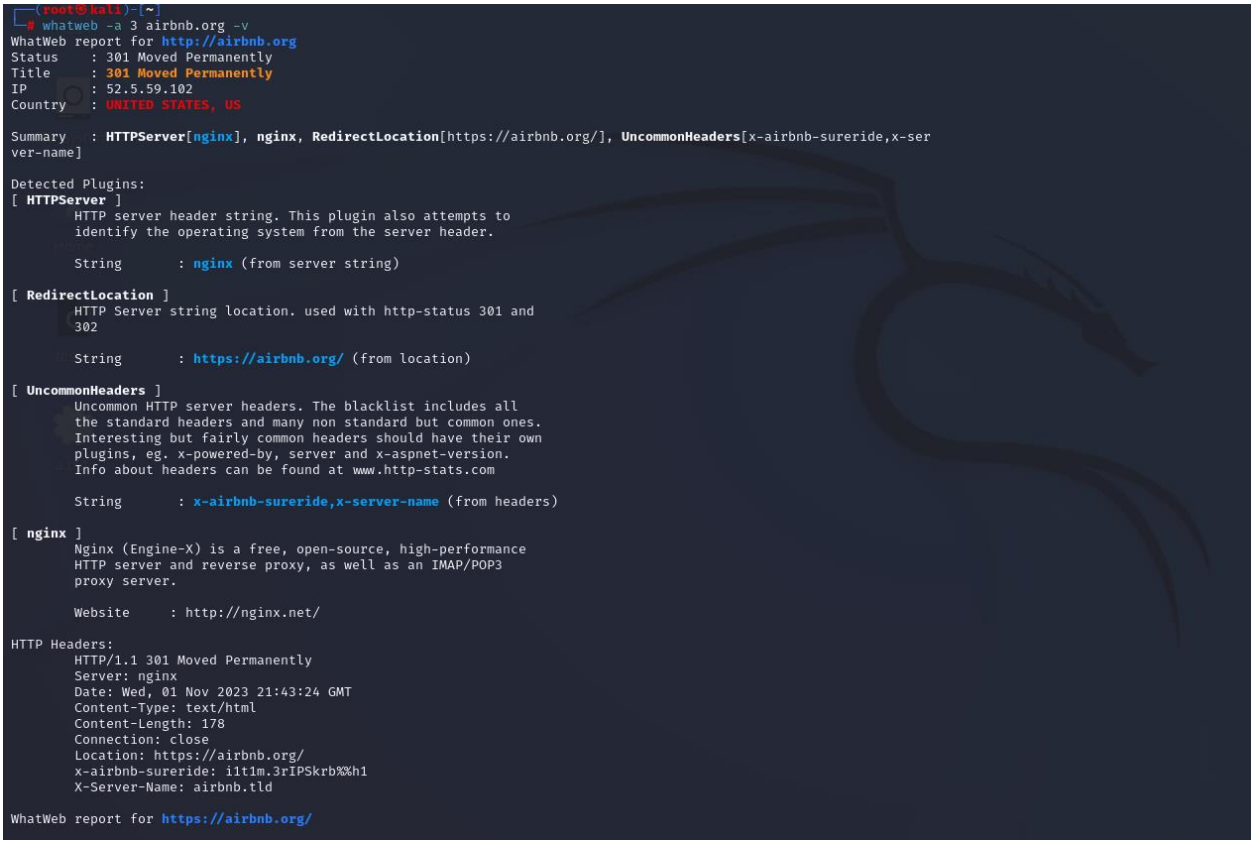
```
Visit MarkMonitor at https://www.markmonitor.com
Contact us at +1.8007459229
In Europe, at +44.02032062220
```

➢ Whatweb

According to Kali Linux, “WhatWeb identifies websites. It recognizes web technologies including content management systems (CMS), blogging platforms, statistic/analytics packages, JavaScript libraries, web servers, and embedded devices.”. This tool is very powerful because we can capture a lot of details using this Whatweb tool. Specially, we can gather information about what type of protection mechanism is used that the targeted domain to protect their web application. But the output information is not sorted well. So, we can use filtering options to gather information in a sorted way.

But I wat a aggressive report.so I try use lev 3 in aggressive.

- Gather information related to http://airbnb.org.



```
WhatWeb report for https://airbnb.org/
Status    : 301 Moved Permanently
Title     : 301 Moved Permanently
IP        : 52.5.59.102
Country   : UNITED STATES, US

Summary   : HTTPServer[nginx], nginx, RedirectLocation[https://www.airbnb.org/], Strict-Transport-Security[max-age=3
1536000; includeSubDomains; preload], UncommonHeaders[x-airbnb-sureride,x-server-name]

Detected Plugins:
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : nginx (from server string)

[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : https://www.airbnb.org/ (from location)

[ Strict-Transport-Security ]
        Strict-Transport-Security is an HTTP header that restricts
        a web browser from accessing a website without the security
        of the HTTPS protocol.

        String       : max-age=31536000; includeSubDomains; preload

[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : x-airbnb-sureride,x-server-name (from headers)

[ nginx ]
        Nginx (Engine-X) is a free, open-source, high-performance
        HTTP server and reverse proxy, as well as an IMAP/POP3
        proxy server.

        Website     : http://nginx.net/

HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Server: nginx
        Date: Wed, 01 Nov 2023 21:43:27 GMT
```

```
HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Server: nginx
        Date: Wed, 01 Nov 2023 21:43:27 GMT
        Content-Type: text/html
        Content-Length: 178
        Connection: close
        Location: https://www.airbnb.org/
        x-airbnb-sureride: 1it1m.lFoLmjCq%%h1
        X-Server-Name: airbnb.tld
        Strict-Transport-Security: max-age=31536000; includeSubDomains; preload

WhatWeb report for https://www.airbnb.org/
Status    : 200 OK
Title     : Airbnb.org
IP        : 23.52.171.241
Country   : UNITED STATES, US

Summary   : Bootstrap, Cookies[_user_attributes,bev,everest_cookie], HTML5, HTTPServer[nginx], nginx, Open-Graph-Pro
tocol[website][138566025676], OpenSearch[/opensearch.xml], Script[application/json], Shopify, Strict-Transport-Secur
ity[max-age=10886400; includeSubdomains], UncommonHeaders[x-instrumentation,x-server-lifecycle-phase,x-kraken-loop-n
ame,content-security-policy,x-envoy-upstream-service-time,x-content-type-options,link,x-airbnb-internal-trace-id,x-s
erved-by,x-server-name,alt-svc,x-airbnb-sureride,cachestatus,server-timing,origin-trial,x-browser-type,x-erf-bev-bev
-is-generated,x-erf-bev-bev], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[1; mode=block]

Detected Plugins:
[ Bootstrap ]
        Bootstrap is an open source toolkit for developing with
        HTML, CSS, and JS.

        Website     : https://getbootstrap.com/

[ Cookies ]
        Display the names of cookies in the HTTP headers. The
        values are not returned to save on space.

        String       : bev
        String       : _user_attributes
        String       : everest_cookie
        String       : _user_attributes
        String       : everest_cookie
        String       : bev

[ HTML5 ]
        HTML version 5, detected by the doctype declaration
```

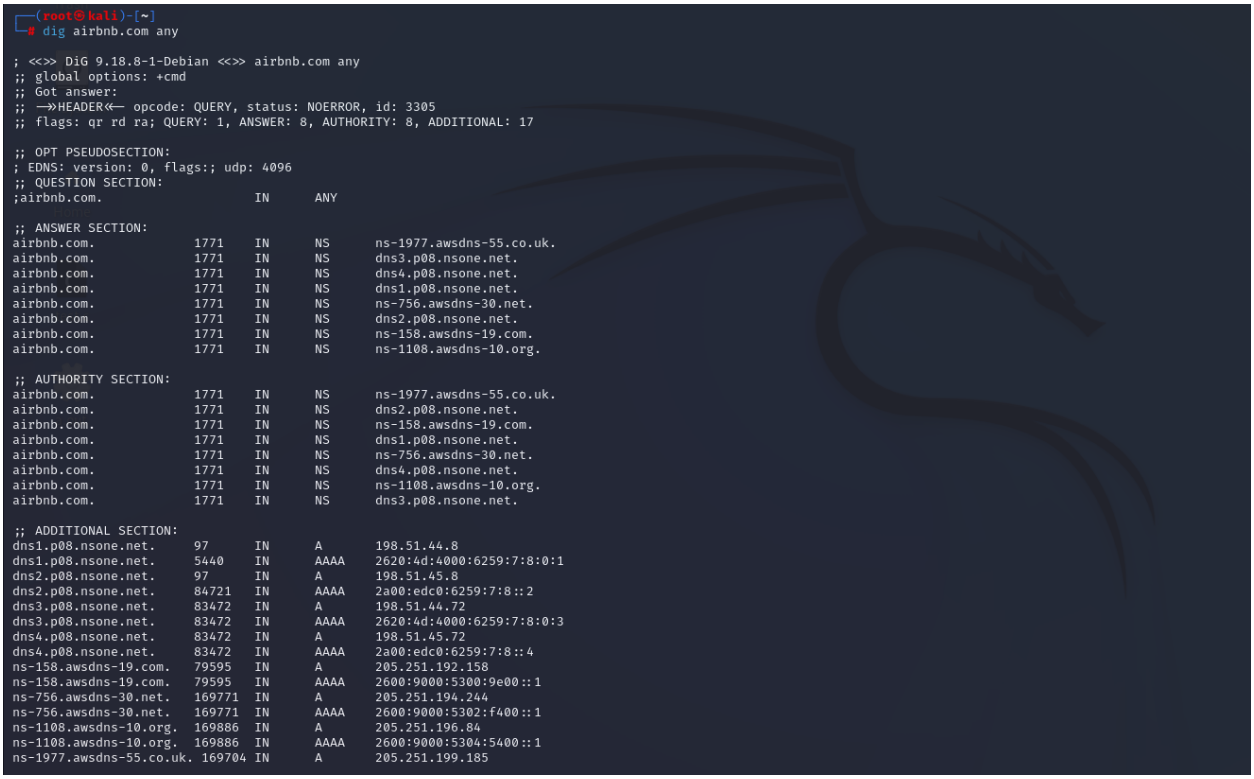
```
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : nginx (from server string)

[ Open-Graph-Protocol ]
        The Open Graph protocol enables you to integrate your Web
        pages into the social graph. It is currently designed for
        Web pages representing profiles of real-world things .
        things like movies, sports teams, celebrities, and
        restaurants. Including Open Graph tags on your Web page,
        makes your page equivalent to a Facebook Page.

        Version      : website
        Module       : 138560025676

[ OpenSearch ]
        This plugin identifies open search and extracts the URL.
        OpenSearch is a collection of simple formats for the
        sharing of search results.

        String       : /opensearch.xml

[ Script ]
        This plugin detects instances of script HTML elements and
        returns the script language/type.

        String       : application/json

[ Shopify ]
        Shopify CMS and ecommerce platform.

        Website     : http://shopify.com/

[ Strict-Transport-Security ]
        Strict-Transport-Security is an HTTP header that restricts
        a web browser from accessing a website without the security
        of the HTTPS protocol.

        String       : max-age=10886400; includeSubdomains

[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
```

```
[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : x-instrumentation,x-server-lifecycle-phase,x-kraken-loop-name,content-security-policy,x-envoy
-upstream-service-time,x-content-type-options,link,x-airbnb-internal-trace-id,x-served-by,x-server-name,alt-svc,x-ai
rbnb-sureride,cachestatus,server-timing,origin-trial,x-browser-type,x-erf-bev-bev-is-generated,x-erf-bev-bev (from h
eaders)

[ X-Frame-Options ]
        This plugin retrieves the X-Frame-Options value from the
        HTTP header. - More Info:
        http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
        aspx

        String       : SAMEORIGIN

[ X-XSS-Protection ]
        This plugin retrieves the X-XSS-Protection value from the
        HTTP header. - More Info:
        http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
        aspx

        String       : 1; mode=block

[ nginx ]
        Nginx (Engine-X) is a free, open-source, high-performance
        HTTP server and reverse proxy, as well as an IMAP/POP3
        proxy server.

        Website     : http://nginx.net/

HTTP Headers:
        HTTP/1.1 200 OK
        Server: nginx
        Content-Type: text/html;charset=utf-8
        x-instrumentation: airbnb
        x-server-lifecycle-phase: running
        status: 200 OK
        x-kraken-loop-name: dot-org-loop
        Cache-Control: no-store, max-age=0, private, must-revalidate
        Content-Security-Policy: connect-src 'self' https: wss://ws.airbnb.com wss://ws.airbnb.org; default-src 'sel
f' https:; font-src 'self' data: https:; frame-src *; img-src 'self' https: data:; media-src 'self' https: blob:; sc
ript-src 'self' https: 'unsafe-eval' 'sha256-rAm9O8JPZLtQmd84zMDzhsG5q35JscESxxcaFL7+DDc=' 'sha256-CZnW0hvLQpXhjRl/r
vattFn8GcIhxi8fcsCstVugtsI=' 'sha256-wTTayjv9vgavK5Y3usV6aqGPwCrn25VsYWYFv7AHK88=' 'sha256-YLUIo40JlmXdE6Sfw9rcwRfWq
RkxTZK7qZ/HL/v/jpQ='; style-src 'self' https: 'unsafe-inline'; worker-src 'self' https: blob:; report-uri /tracking/
csp?controller=dot-org-loop&action=%2F&req_uuid=b8b2d7f7-cba6-4690-a6fe-9ef1d6241256&version=sha%3Df2c66289fa87&repo
```

```
        Content-Security-Policy: connect-src 'self' https: wss://ws.airbnb.com wss://ws.airbnb.org: default-src 'sel
f' https:; font-src 'self' data: https:; frame-src *; img-src 'self' https: data:; media-src 'self' https: blob:; sc
ript-src 'self' https: 'unsafe-eval' 'sha256-rAm9O8JPZLtQmd84zMDzhsG5q35JscE5xxcaFL7+DDc=' 'sha256-CZnW0hvLQpXbjRl/r
vattFn8GcIhxi8fcsCstVugtsI=' 'sha256-wTTayjv9vgavK5Y3usV6aqGPwCrn25VsYWYFv7AHK88=' 'sha256-YLUIo40JlmXdE6Sfw9rcwRfWq
RkxTZK7qZ/HL/v/jpQ=' 'sha256-kAIGpoO6IqbiYjtXfiI9AtTkkWE=' 'sha256-YLUIo40JlmXdE6Sfw9rcwRfWqRkxTZK7qZ/HL/v/jpQ=';
 style-src 'self' https: 'unsafe-inline'; worker-src 'self' https: blob:; report-uri /tracking/csp?controller=dot-
org-loop&action=%2F&req_uuid=b8b2d7f7-cba6-4690-a6fe-9ef1d6241256&version=sha%3Df2c66289fa87&report_only=false; repo
rt-to /tracking/csp?controller=dot-org-loop&action=%2F&req_uuid=b8b2d7f7-cba6-4690-a6fe-9ef1d62412566version=sha%3Df2c66289fa87&repo
rt_only=false; report-to /tracking/csp?controller=dot-org-loop&action=%2F&req_uuid=b8b2d7f7-cba6-4690-a6fe-9ef1d6241
2566version=sha%3Df2c66289fa87&report_only=false
        x-frame-options: SAMEORIGIN
        x-envoy-upstream-service-time: 119
        x-xss-protection: 1; mode=block
        ETag: W/"231d5-kAIGpoO6IqbiYjtXfiI9AtTkkWE--gzip"
        x-content-type-options: nosniff
        Link: <https://a0.muscache.com/airbnb/static/packages/common-d60efc079a4a5061d9e359d59fdeaf87.css>;rel=prelo
ad;as=style;crossorigin=anonymous,<https://a0.muscache.com/airbnb/static/packages/dls/dls-lite_cereal-118e5a203377de
a19a81017b1794f159.css>;rel=preload;as=style;crossorigin=anonymous,<https://a0.muscache.com/airbnb/static/airbnb-dls
-web/build/fonts/Airbnb_Cereal-Book-9a1c9cca9bb3d65fefa2aa487617805e.woff2>;rel=preload;as=font;type=font/woff2;cros
sorigin=anonymous,<https://a0.muscache.com/airbnb/static/airbnb-dls-web/build/fonts/Airbnb_Cereal-Medium-50fc004b308
2375f12ff0cfb67bf8e56.woff2>;rel=preload;as=font;type=font/woff2;crossorigin=anonymous,<https://a0.muscache.com/airb
nb/static/airbnb-dls-web/build/fonts/Airbnb_Cereal-Bold-bdfb98485e7836ba31b456f65cded088.woff2>;rel=preload;as=font;
type=font/woff2;crossorigin=anonymous
        x-airbnb-internal-trace-id: 2yzm9zfPrAr1yUd8pVaRCw==
        Strict-Transport-Security: max-age=10886400; includeSubdomains
        X-Served-By: monorail
        X-Server-Name: www.airbnb.org
        Vary: Accept-Encoding
        Date: Wed, 01 Nov 2023 21:43:31 GMT
        Transfer-Encoding:  chunked
        Connection: close
        Connection: Transfer-Encoding
        Set-Cookie: bev=1698875010_OWUyNzczYjc5NmM1; Domain=.airbnb.org; Path=/; Expires=Fri, 31 Oct 2025 21:43:30 G
MT; Secure
        Set-Cookie: _user_attributes=%7B%22curr%22%3A%22LKR%22%2C%22device_profiling_session_id%22%3A%221698875010--
2296b754e351603e6f89d658%22%2C%22giftcard_profiling_session_id%22%3A%221698875010--3391dfed9e253061fe31e3dc%22%2C%22
reservation_profiling_session_id%22%3A%221698875010--842ce3a8a4ca2d292eaa84f0%22%7D; Domain=.airbnb.org; Path=/; Exp
ires=Sat, 01 Nov 2025 21:43:30 GMT; Secure
        Set-Cookie: everest_cookie=1698875010.VTP3tqwchdPm7Y5ItTjK.Hfqk-UQH8Zo6G6iESLjayv2lY8GsYuwvdcnUmmiovQ8; Doma
in=.airbnb.org; Path=/; Expires=Sat, 31 Oct 2026 21:43:30 GMT; Secure
        Set-Cookie: _user_attributes=%7B%22device_profiling_session_id%22%3A%221698875010--2296b754e351603e6f89d658%
22%2C%22giftcard_profiling_session_id%22%3A%221698875010--3391dfed9e253061fe31e3dc%22%2C%22reservation_profiling_ses
sion_id%22%3A%221698875010--842ce3a8a4ca2d292eaa84f0%22%2C%22curr%22%3A%22LKR%22%7D; Domain=.airbnb.org; Path=/; Exp
ires=Sat, 01 Nov 2025 21:43:30 GMT; Secure
        Set-Cookie: everest_cookie=1698875010.VTP3tqwchdPm7Y5ItTjK.Hfqk-UQH8Zo6G6iESLjayv2lY8GsYuwvdcnUmmiovQ8; Doma
in=.airbnb.org; Path=/; Expires=Sat, 31 Oct 2026 21:43:30 GMT; Secure
        Set-Cookie: bev=1698875010_OWUyNzczYjc5NmM1; expires=Fri, 31-Oct-2025 21:43:31 GMT; path=/; domain=.airbnb.o
rg; secure
        Alt-Svc: h3=":443"; ma=93600
        x-airbnb-sureride: c1a1o.0.afa83b17.1698875010.1bfc6ff9%%i1c1o%%t1d1o.2yzm9zfPrAr1yUd8pVaRCw==%%h1
        Cachestatus: origin
        Server-Timing: cdn-cache; desc=NO-STORE, edge; dur=357, origin; dur=127
        origin-trial: AkOekvxwprBLSP7I2nhyRn5yZGt9lTJN6UIYziFKVYg5OhlzmlNDciWbBWkEQ5TYPz+aqsuIUT2pPEjPUD5dFAsAAABney
JvcmlnaW4iOiJodHRwczovL2FpcmJuYi5jb206NDQzIiwiZmVhdHVyZSI6IlByaW9yaXR5SGludHNBUEkiLCJleHBpcnkiOjE2NDc5OTM1OTksImlzU3
ViZG9tYWluIjp0cnVlfQ==
        x-browser-type: unknown
        x-erf-bev-bev-is-generated: 1
        x-erf-bev-bev: 1698875010_OWUyNzczYjc5NmM1
```

➢ Dig

Domain Information Groper (dig) is used for gathering information relevant to Domain Name System (DNS). This command is also the same as the nslookup command. But dig command present the information sorted way than the nslookup command.

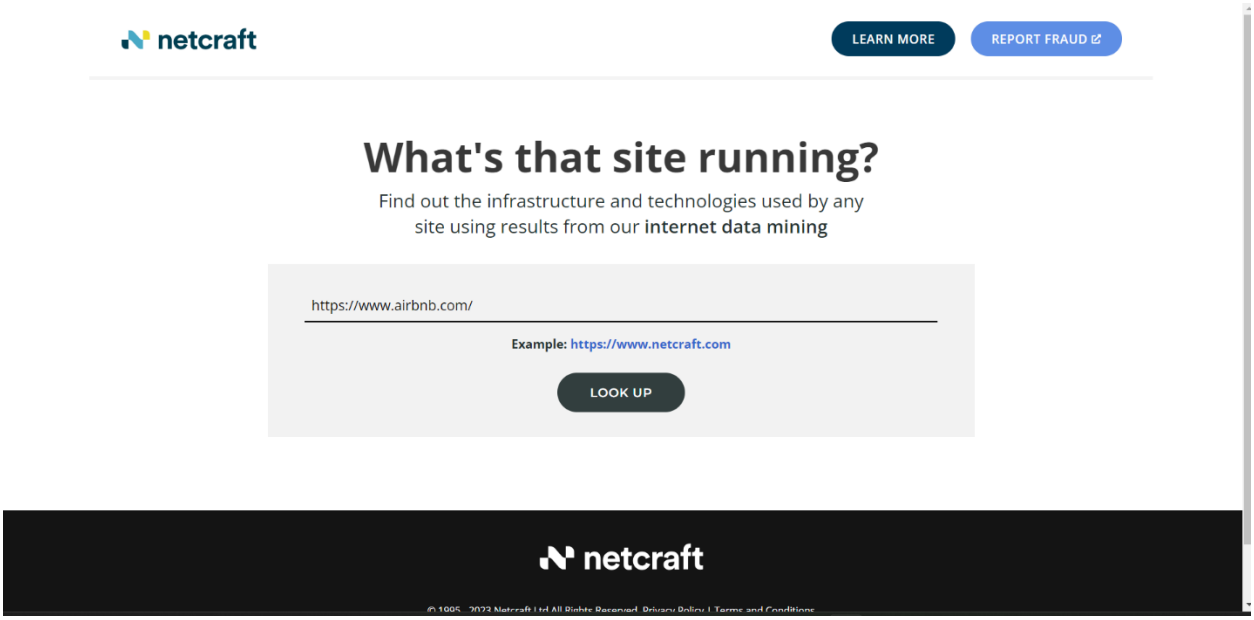


```
┌──(root㉿kali)-[~]
└─# dig airbnb.com any

; <<>> DiG 9.18.8-1-Debian <<>> airbnb.com any
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3305
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 8, ADDITIONAL: 17

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;airbnb.com.                    IN      ANY

;; ANSWER SECTION:
airbnb.com.             1771    IN      NS      ns-1977.awsdns-55.co.uk.
airbnb.com.             1771    IN      NS      dns3.p08.nsone.net.
airbnb.com.             1771    IN      NS      dns4.p08.nsone.net.
airbnb.com.             1771    IN      NS      dns1.p08.nsone.net.
airbnb.com.             1771    IN      NS      ns-756.awsdns-30.net.
airbnb.com.             1771    IN      NS      dns2.p08.nsone.net.
airbnb.com.             1771    IN      NS      ns-158.awsdns-19.com.
airbnb.com.             1771    IN      NS      ns-1108.awsdns-10.org.

;; AUTHORITY SECTION:
airbnb.com.             1771    IN      NS      ns-1977.awsdns-55.co.uk.
airbnb.com.             1771    IN      NS      dns2.p08.nsone.net.
airbnb.com.             1771    IN      NS      ns-158.awsdns-19.com.
airbnb.com.             1771    IN      NS      dns1.p08.nsone.net.
airbnb.com.             1771    IN      NS      ns-756.awsdns-30.net.
airbnb.com.             1771    IN      NS      dns4.p08.nsone.net.
airbnb.com.             1771    IN      NS      ns-1108.awsdns-10.org.
airbnb.com.             1771    IN      NS      dns3.p08.nsone.net.

;; ADDITIONAL SECTION:
dns1.p08.nsone.net.     97      IN      A       198.51.44.8
dns1.p08.nsone.net.     5440    IN      AAAA    2620:4d:4000:6259:7:8:0:1
dns2.p08.nsone.net.     97      IN      A       198.51.45.8
dns2.p08.nsone.net.     84721   IN      AAAA    2a00:edc0:6259:7:8::2
dns3.p08.nsone.net.     83472   IN      A       198.51.44.72
dns3.p08.nsone.net.     83472   IN      AAAA    2620:4d:4000:6259:7:8:0:3
dns4.p08.nsone.net.     83472   IN      A       198.51.45.72
dns4.p08.nsone.net.     83472   IN      AAAA    2a00:edc0:6259:7:8::4
ns-158.awsdns-19.com.   79595   IN      A       205.251.192.158
ns-158.awsdns-19.com.   79595   IN      AAAA    2600:9000:5300:9e00::1
ns-756.awsdns-30.net.   169771  IN      A       205.251.194.244
ns-756.awsdns-30.net.   169771  IN      AAAA    2600:9000:5302:f400::1
ns-1108.awsdns-10.org.  169886  IN      A       205.251.196.84
ns-1108.awsdns-10.org.  169886  IN      AAAA    2600:9000:5304:5400::1
ns-1977.awsdns-55.co.uk. 169704 IN      A       205.251.199.185
```

```
;; Query time: 52 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (TCP)
;; WHEN: Fri Nov 03 00:53:47 CDT 2023
;; MSG SIZE  rcvd: 726
```

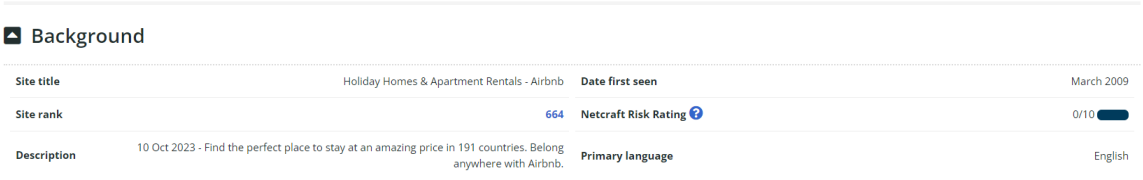
➢ Netcraft

Netcraft (https://sitereport.netcraft.com/) is an online web tool used to gather information related to technologies utilized in web application development. This tool is helping to identify out-of-date software modules used to develop the web application. These outdated software modules can be vulnerable to exploitation.

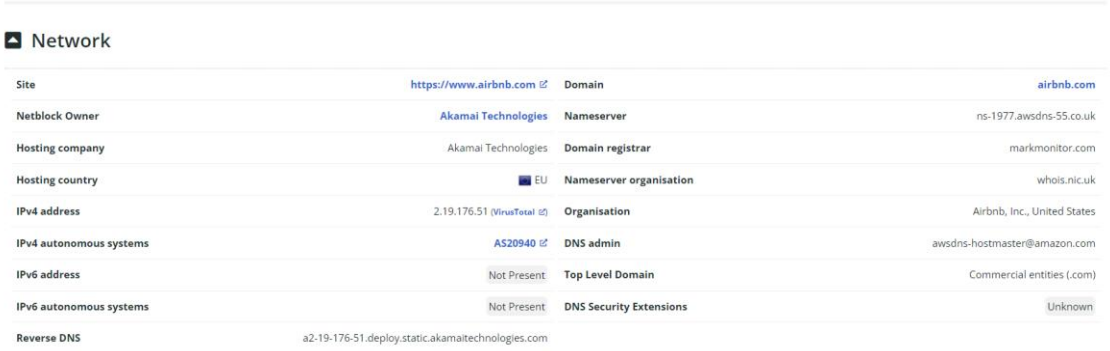


This is the main interface of the Netcraft tool. We must enter the domain name to get the details from this tool.

- Gather details about the Background of the targeted domain.



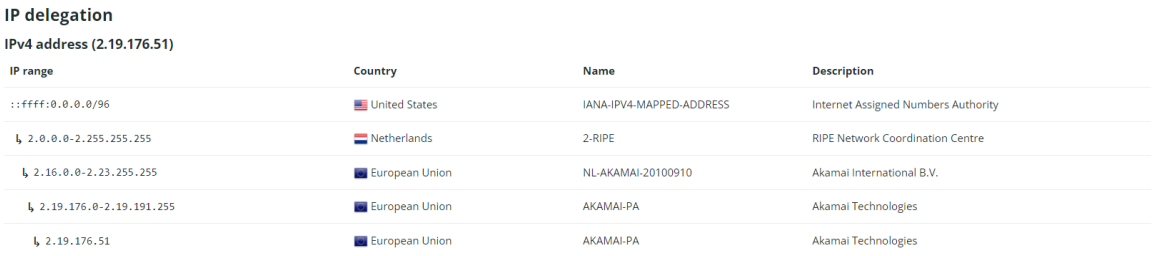
- Gather details about the Network of the targeted domain.



Network

Site	https://www.airbnb.com	Domain	airbnb.com
Netblock Owner	Akamai Technologies	Nameserver	ns-1977.awsdns-55.co.uk
Hosting company	Akamai Technologies	Domain registrar	markmonitor.com
Hosting country	EU	Nameserver organisation	whois.nic.uk
IPv4 address	2.19.176.51 (VirusTotal)	Organisation	Airbnb, Inc., United States
IPv4 autonomous systems	AS20940	DNS admin	awsdns-hostmaster@amazon.com
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	Unknown
Reverse DNS	a2-19-176-51.deploy.static.akamaitechnologies.com		

- Gather information regarded to IP Delegation of the targeted domain.



IP delegation

IPv4 address (2.19.176.51)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
2.0.0.0-2.255.255.255	Netherlands	2-RIPE	RIPE Network Coordination Centre
2.16.0.0-2.23.255.255	European Union	NL-AKAMAI-20100910	Akamai International B.V.
2.19.176.0-2.19.191.255	European Union	AKAMAI-PA	Akamai Technologies
2.19.176.51	European Union	AKAMAI-PA	Akamai Technologies

- Gather the information about Hosting History, Sender Policy Framework, and DMARC of the targeted domain.

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Akamai Technologies	92.122.164.45	Linux	nginx	7-Mar-2021
Fastly, Inc. PO Box 78266 San Francisco CA US 94107	151.101.17.254	Linux	nginx	17-Jul-2020
Fastly, Inc. PO Box 78266 San Francisco CA US 94107	199.232.57.254	Linux	nginx	29-Jun-2020
Fastly, Inc. PO Box 78266 San Francisco CA US 94107	151.101.17.254	Linux	nginx	18-Jun-2020
Fastly, Inc. PO Box 78266 San Francisco CA US 94107	151.101.61.254	Linux	nginx	21-Apr-2020
Fastly, Inc. PO Box 78266 San Francisco CA US 94107	151.101.17.254	Linux	nginx	23-Feb-2019
Fastly, Inc. PO Box 78266 San Francisco CA US 94107	151.101.61.254	Linux	nginx	9-Jan-2018
Akamai Technologies	2.17.148.52	Linux	nginx/1.7.12	3-Jun-2017
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	173.222.129.25	Linux	nginx/1.7.12	25-Mar-2017
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.166.123	Linux	nginx/1.7.12	19-Oct-2016

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of **rules**. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see **open-spf.org**.

Warning: It appears that this host does not have an SPF record. There may be an SPF record on airbnb.com: Check the **site report**.

Setting up an SPF record helps prevent the delivery of forged emails from your domain. Please note that an SPF record will only protect the domain it is added to and not any **mail-enabled subdomains**. It is recommended to add an SPF record to any subdomain with an MX record.

DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see **dmarc.org**.

This host does not have a DMARC record. There may be a DMARC record on the site report for airbnb.com: Check the **site report**.

- Gather the information about Site Technology.

Site Technology (fetched 24 days ago)

HTTP Accelerator

A web accelerator is a proxy server that reduces web site access times.

Technology	Description	Popular sites using this technology
Envoy	Open source proxy	www.ebay.co.uk, www.ebay.com, www.researchgate.net

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
XML	*No description*	www.xvideos.com, www.virustotal.com, www.qwant.com

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	www.linkedin.com, t.co

Content Delivery Network

A content delivery network or content distribution network (CDN) is a large distributed system of servers deployed in multiple data centers in the Internet. The goal of a CDN is to serve content to end-users with high availability and high performance.

Technology	Description	Popular sites using this technology
Akamai	Web Content Delivery service provider	www.infobae.com, www.reuters.com, www.npr.org

Search

A web search engine is a software that is designed to search for information on the World Wide Web or on a specific site.

Technology	Description	Popular sites using this technology
Custom Search Engine	Google Custom Search Engine	www.aliexpress.com, www.pinterest.com, www.ecosia.org

Character Encoding

A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.

Technology	Description	Popular sites using this technology
UTF8	UCS Transformation Format 8 bit	

HTTP Compression

HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.

Technology	Description	Popular sites using this technology
Gzip Content Encoding	Gzip HTTP Compression protocol	www.nfl.com, www.seznam.cz, www.wildberries.ru

Web Browser Targeting

Web browser targeting enables software applications to make use of specific functions of the browser as well as optimizing the application for specific browser versions.

Technology	Description	Popular sites using this technology
X-Content-Type-Options	Browser MIME type sniffing is disabled	www.reddit.com, mail-redir.mention.com, accounts.google.com
Strict Transport Security	Web security policy mechanism whereby a web server declares that complying user agents are to interact with it using only secure HTTP connections	outlook.office.com, teams.microsoft.com
X-Frame-Options Same Origin	Do not allow this site to be rendered within an iframe	www.canva.com, www.startpage.com, www.tiktok.com
Strict-Transport-Security (including subdomains)	*No description*	www.binance.com, arco.okta.com
Content Security Policy Report	Detect, mitigate and report attacks in the browser	www.amazon.de, www.amazon.co.uk, www.bbc.co.uk
X-XSS-Protection Block	Block pages on which cross-site scripting is detected	
Content Security Policy	Detect and mitigate attacks in the browser	www.baidu.com

Doctype

A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

Technology	Description	Popular sites using this technology
HTML5	Latest revision of the HTML standard, the main markup language on the web	

HTML 5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

Technology	Description	Popular sites using this technology
Viewport meta tag	HTML5 tag usually used for mobile optimization	

CSS Usage

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

Technology	Description	Popular sites using this technology
External	Styles defined within an external CSS file	www.instagram.com, www.deepl.com, www.amazon.com
CSS Media Query	*No description*	www.netflix.com, www.twitch.tv, www.facebook.com

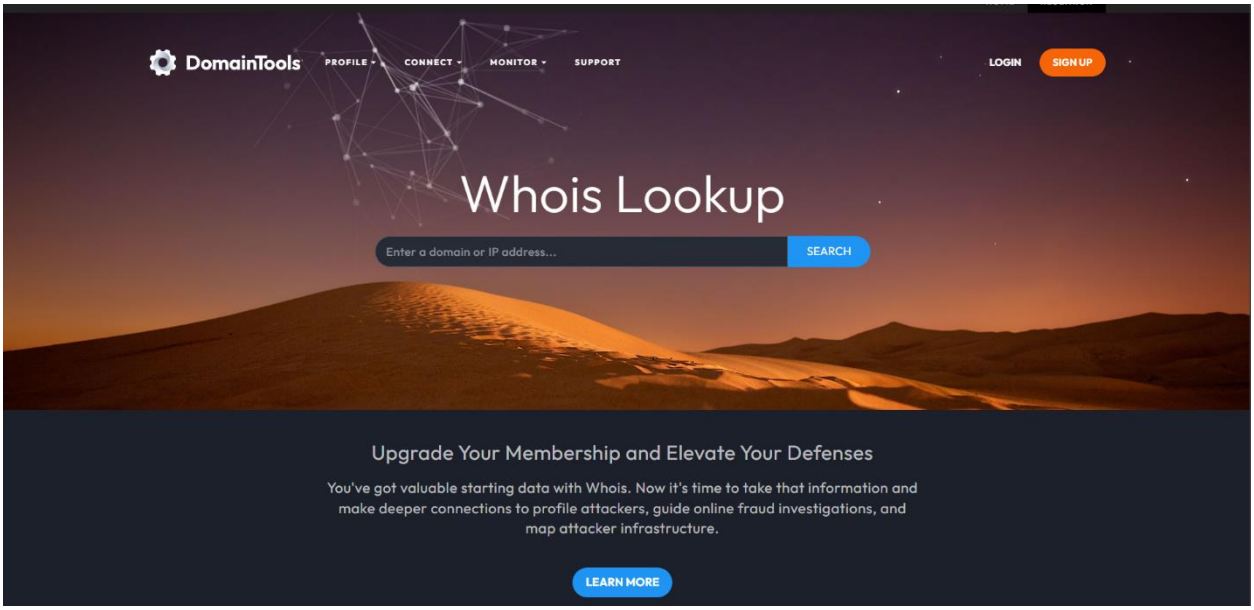
- Gather the information about SSL/TLS

SSL/TLS

Assurance	Organisation validation	**Perfect Forward Secrecy**	Yes
Common name	www.airbnb.com	**Supported TLS Extensions**	RFC8446 supported versions, RFC8446 key share, RFC4366 server name, RFC4492 elliptic curves, RFC7301 application-layer protocol negotiation, RFC4366 status request
Organisation	Airbnb, Inc.	**Application-Layer Protocol Negotiation**	h2
State	California	**Next Protocol Negotiation**	Not Present
Country	US	**Issuing organisation**	DigiCert Inc
Organisational unit	Not Present	**Issuer common name**	DigiCert TLS RSA SHA256 2020 CA1
Subject Alternative Name	www.airbnb.com, zu.airbnb.com, www.airbnb.si, www.airbnb.se, www.airbnb.rs, www.airbnb.pt, www.airbnb.pl, www.airbnb.no, www.airbnb.nl, www.airbnb.mx, www.airbnb.me and 86 more	**Issuer unit**	Not Present
Validity period	From Feb 22 2023 to Mar 15 2024 (12 months, 3 weeks)	**Issuer location**	Not Present
Matches hostname	Yes	**Issuer country**	US
Server	nginx	**Issuer state**	Not Present
Public key algorithm	rsaEncryption	**Certificate Revocation Lists**	http://crl3.digicert.com/DigiCertTLSRSASHA2562020CA1-4.crl http://crl4.digicert.com/DigiCertTLSRSASHA2562020CA1-4.crl
Protocol version	TLSv1.3	**Certificate Hash**	ViHG0nultVeugZHufrENoQHwja8
Public key length	2048	**Public Key Hash**	a54142f88f074b2e8595e80706eb4817e30fee81ae88edf897aa2f0f6bd5d81a
Certificate check	ok	**OCSP servers**	http://ocsp.digicert.com - *100% uptime in the past 24 hours* Performance Graph
Signature algorithm	sha256WithRSAEncryption	**OCSP stapling response**	Certificate valid
Serial number	0x0161814b7dfe0f30f706b8baa6f6ef00	**OCSP data generated**	Nov 1 06:21:02 2023 GMT
Cipher	TLS_AES_256_GCM_SHA384	**OCSP data expires**	Nov 8 05:21:02 2023 GMT
Version number	0x02		

➢ Whois lookup

Whois Lookup (https://whois.domaintools.com/) is an online web tool used to gather information about the hosted company, owner of a target, Server Type, and location of servers.



- Gather the IP information using the targeted domain IP address.

Whois Record for AiRbNb.com

— Domain Profile

Registrar	MarkMonitor, Inc. MarkMonitor Inc. IANA ID: 292 URL: http://www.markmonitor.com Whois Server: whois.markmonitor.com abusecomplaints@markmonitor.com (p) +1.2086851750
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	5,568 days old Created on 2008-08-05 Expires on 2024-08-05 Updated on 2023-08-23
Name Servers	DNS1.P08.NSONE.NET (has 3,188,630 domains) DNS2.P08.NSONE.NET (has 3,188,630 domains) DNS3.P08.NSONE.NET (has 3,188,630 domains) DNS4.P08.NSONE.NET (has 3,188,630 domains) NS-1108.AWSDNS-10.ORG (has 53,770 domains) NS-158.AWSDNS-19.COM (has 2,044 domains) NS-1977.AWSDNS-55.CO.UK (has 257 domains) NS-756.AWSDNS-30.NET (has 38 domains)

IP Address	184.28.93.19 - 573 other sites hosted on this server
IP Location	- Washington - Seattle - Akamai Technologies Inc.
ASN	AS20940 AKAMAI-ASN1 Akamai International B.V., NL (registered Jul 10, 2001)
Domain Status	Registered And No Website
IP History	370 changes on 370 unique IP addresses over 15 years
Registrar History	2 registrars
Hosting History	3 changes on 4 unique name servers over 15 years

Whois Record (last updated on 2023-11-03)

```
Domain Name: airbnb.com
Registry Domain ID: 1512196199_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2023-08-23T22:03:11+00:00
        2023-08-23
Creation Date: 2008-08-05T07:29:00+00:00
        2008-08-05
Registrar Registration Expiration Date: 2024-08-05T00:00:00+00:00
        2024-08-05
Registrar: MarkMonitor, Inc.
        MarkMonitor Inc.
Sponsoring Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Status:
        clientDeleteProhibited
        clientTransferProhibited
        clientUpdateProhibited
        serverDeleteProhibited
        serverTransferProhibited
        serverUpdateProhibited
Registry Registrant ID:
Registrant Name:
Registrant Organization: Airbnb, Inc.
Registrant Street:
Registrant City:
Registrant State/Province: CA
Registrant Postal Code:
Registrant Country: US
Registrant Phone:
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
```

```
Registrant Fax Ext:
Registrant Email: REDACTED FOR PRIVACY (DT)
Registry Admin ID:
Admin Name:
Admin Organization: Airbnb, Inc.
Admin Street:
Admin City:
Admin State/Province: CA
Admin Postal Code:
Admin Country: US
Admin Phone:
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: REDACTED FOR PRIVACY (DT)
Registry Tech ID:
Tech Name:
Tech Organization: Airbnb, Inc.
Tech Street:
Tech City:
Tech State/Province: CA
Tech Postal Code:
Tech Country: US
Tech Phone:
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: REDACTED FOR PRIVACY (DT)
Registry Billing ID:
Billing Name:
Billing Organization:
Billing Street:
Billing City:
Billing State/Province:
Billing Postal Code:
Billing Country:
Billing Phone:
Billing Phone Ext:
Billing Fax:
```

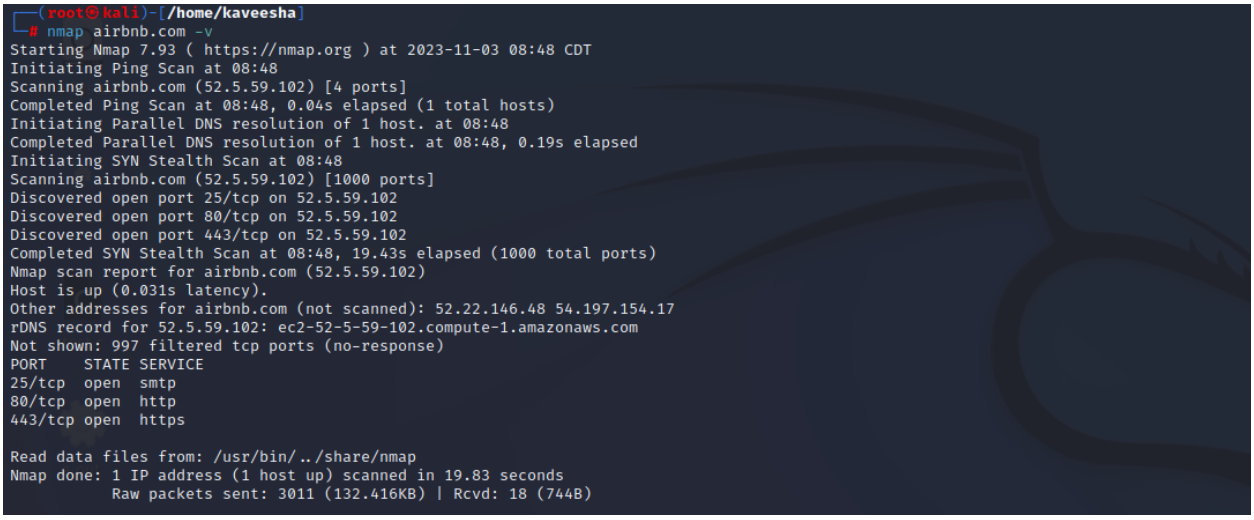
```
Billing Fax:
Billing Fax Ext:
Billing Email:
Nameservers:
        dns1.p08.nsone.net
        dns2.p08.nsone.net
        dns3.p08.nsone.net
        dns4.p08.nsone.net
        ns-1108.awsdns-10.org
        ns-158.awsdns-19.com
        ns-1977.awsdns-55.co.uk
        ns-756.awsdns-30.net
DNSSEC: unsigned
```

2. Active information gathering tools.

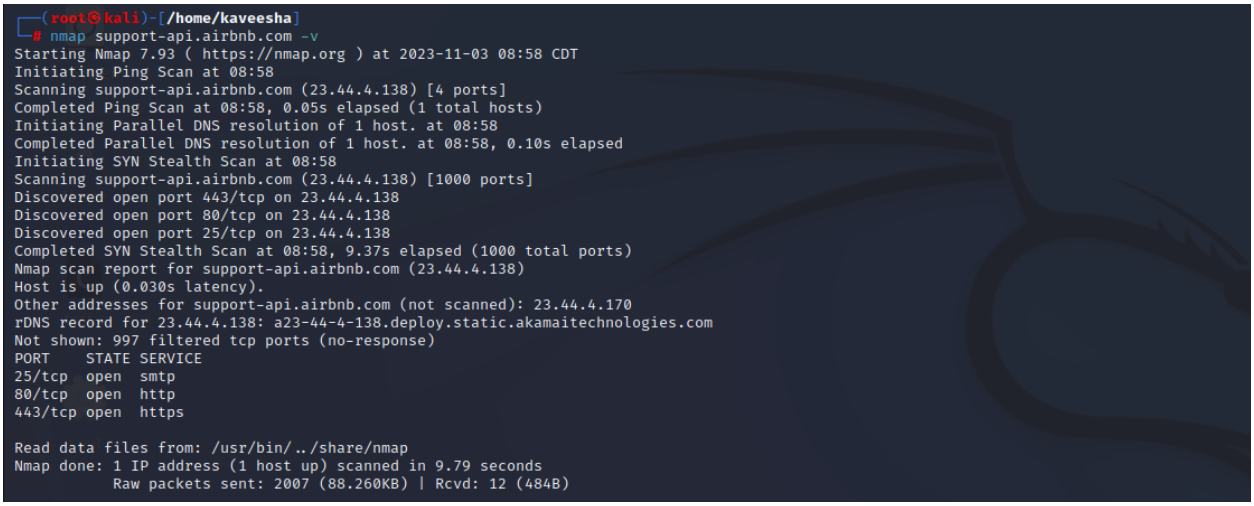
➢ Nmap

Nmap is a tool used to recognize the state of ports, the host is up and running or not, and much other useful information can gather using this tool. Nmap tool also can be used to scan vulnerabilities inside the targeted domain. But now I use this tool only to gather information about the open ports or those ports are filtered, closed, or unfiltered. So, using the Nmap tool to execute SYN scan to gather the details about the open port of the targeted domains.

- Gather open port information about the www.airbnb.com web domain.



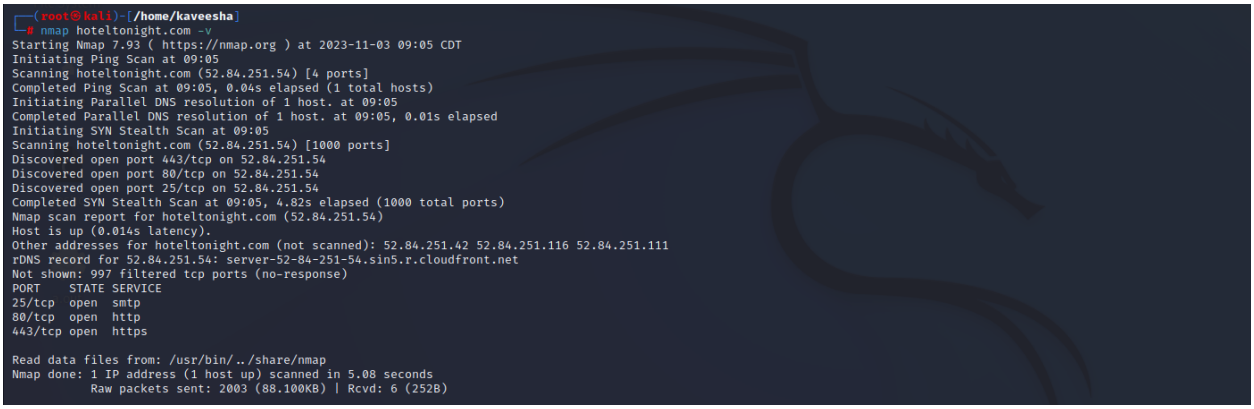
- Gather open port information about the support-api.airbnb.com web domain.



- Gather open port information about the one.airbnb.com web domain.

- Gather open port information about the next.airbnb.com web domain.

- Gather open port information about the hoteltonight.com web domain.



➢ Dmitry

Dmitry is a collection of information-gathering tools. Because of that, this tool is a combination or package of tools. Using this tool, we can gather details related to Whois lookup web tool information, Netcraft information, and open port details. Because this tool gathers information about open ports, Dmitry is an Active information gathering tool.

```
┌──(kaveesha㉿kali)-[~]
└─$ dmitry -h
Deepmagic Information Gathering Tool
"There be some deep magic going on"

dmitry: invalid option -- 'h'
Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
  -o     Save output to %host.txt or to file specified by -o file
  -i     Perform a whois lookup on the IP address of a host
  -w     Perform a whois lookup on the domain name of a host
  -n     Retrieve Netcraft.com information on a host
  -s     Perform a search for possible subdomains
  -e     Perform a search for possible email addresses
  -p     Perform a TCP port scan on a host
* -f     Perform a TCP port scan on a host showing output reporting filtered ports
* -b     Read in the banner received from the scanned port
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed
```

- Gathering Information related to deepmagic according to Airbnb.com domain IP address.

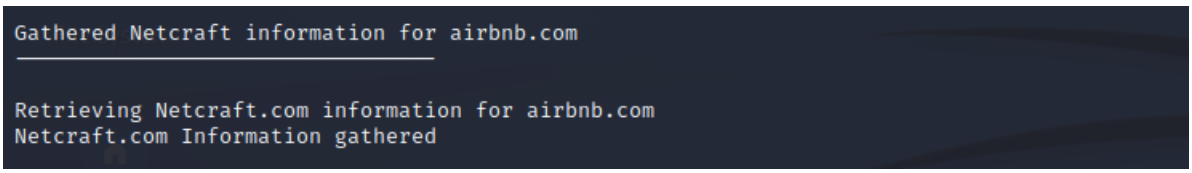
```
┌──(kaveesha㉿kali)-[~]
└─$ dmitry airbnb.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:52.5.59.102
HostName:airbnb.com

Gathered Inet-whois information for 52.5.59.102
---------------------------------


inetnum:        52.0.0.0 - 52.144.63.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        ------------------------------------------------------
remarks:
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:
remarks:        LACNIC (Latin America and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks:        ------------------------------------------------------
country:        EU # Country is really world wide
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
status:         ALLOCATED UNSPECIFIED
mnt-by:         RIPE-NCC-HM-MNT
created:        2019-01-07T10:46:10Z
last-modified:  2019-01-07T10:46:10Z
source:         RIPE
```

```
role:           Internet Assigned Numbers Authority
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
nic-hdl:        IANA1-RIPE
remarks:        For more information on IANA services
remarks:        go to IANA web site at http://www.iana.org.
mnt-by:         RIPE-NCC-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2001-09-22T09:31:27Z
source:         RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.108 (DEXTER)
```

- Gathering Information related to Inic-whois according to Airbnb.com domain IP address.

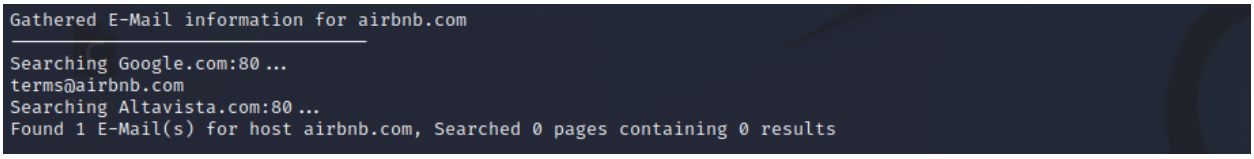
```
Gathered Inic-whois information for airbnb.com
---------------------------------------------

   Domain Name: AIRBNB.COM
   Registry Domain ID: 1512196199_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2023-08-23T20:10:06Z
   Creation Date: 2008-08-05T07:29:00Z
   Registry Expiry Date: 2024-08-05T07:29:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: DNS1.P08.NSONE.NET
   Name Server: DNS2.P08.NSONE.NET
   Name Server: DNS3.P08.NSONE.NET
   Name Server: DNS4.P08.NSONE.NET
   Name Server: NS-1108.AWSDNS-10.ORG
   Name Server: NS-158.AWSDNS-19.COM
   Name Server: NS-1977.AWSDNS-55.CO.UK
   Name Server: NS-756.AWSDNS-30.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2023-11-03T16:39:53Z <<<
```

- Gathering Information related to netcraft according to Airbnb.com domain IP address.

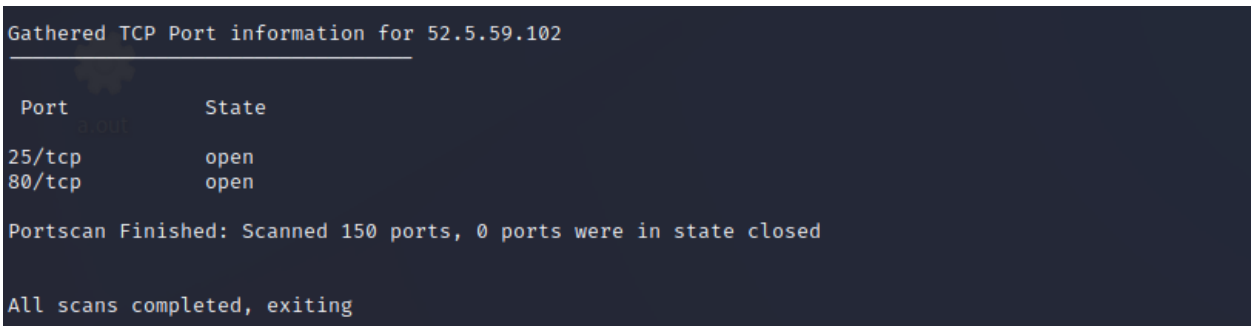


- Gathering Information related to subdomains according to Airbnb.com domain IP address.

- Gathering Information related to E-mail according to Airbnb.com domain IP address.



- Gathering Information related to TCP Port according to airbnb domain IP address.



Planning and analysis

After the information gathering stage, we need to analyze those details to plan what we focused on next stagers. The planning stage is very essential because vulnerability detection is a time-consuming process and with the plan, we can do vulnerability detection in a targeted way. So, we can save our time and vulnerability detection also can be done in a very efficient manner.

So, after the information gathering process that the collected data can be sorted down according to the technical details such as, Web server details, Application server details, and Database server details. And also, that the state of the ports and the HTTP protection methods are the details focused on to execute the vulnerability scan.

- Technical details
  - ✓ **Web server**
    - HTTPS server is Nginx.
      - Airbnb.com(version)
    - HTTP server is nginx.
      - support-api.airbnb.com(version not defind)
      - Hoteltonight.com(version not defind)
    - http server is varnish.
      - hoteltonight.com
    - http/https server is Cloudflare.
      - airbnbhelp.com
  - ✓ **application server**
    - python
      - hoteltonight.com
    - php
      - open.airbnb.com
- ❖ Open ports details are in the Nmap scan report done in the information gathering stage.
- ❖ HTTP security details are in the Wahtweb scan report done in the information gathering stage.

After that select vulnerability scanning tools according to the gathered information and plan the vulnerability scanning according to the information analysis details.

Vulnerability detection

Vulnerability Detection is a very important stage in Bug Bounty assessment. Because before moving to the penetration testing stage we need to identify vulnerabilities in the system. According to Balbix, “Vulnerability scanning is the process of identifying security weaknesses and flaws in the system.”

There are two vulnerability detection methods. They are the automated scanning method and the manual scanning method. I use both methods to detect vulnerabilities in the targeted system. Most of the tools can scan vulnerabilities in the system for two methods. Manual scanning is something like a filtered way of scanning and automated scanning is go through all subdomains in the system and scans all vulnerabilities in the system. The automated scanning method is very easy, but it is a time-consuming method. Because manual scanning is an efficient way of vulnerability detection method.

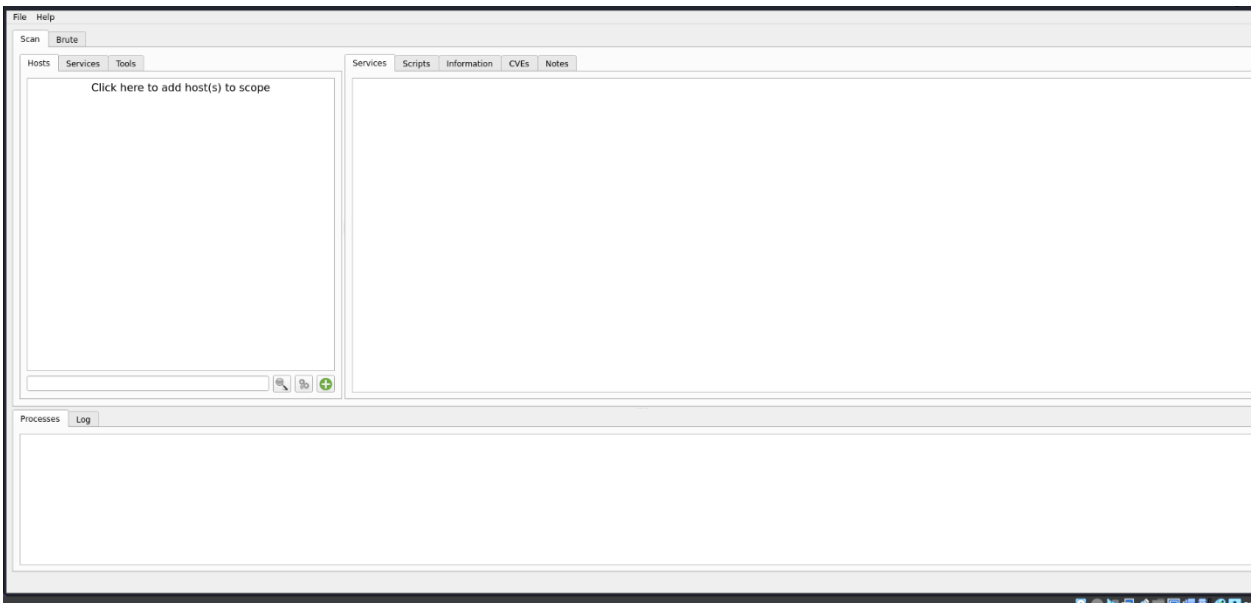
So, detecting those vulnerabilities can be done using the Vulnerability Detection tools. There are a lot of open-source and paid tools. They are,

- Legion
- Nikto
- Nmap
- Arachni
- Uniscan
- Netsparker
- Nessus
- Owasp zap

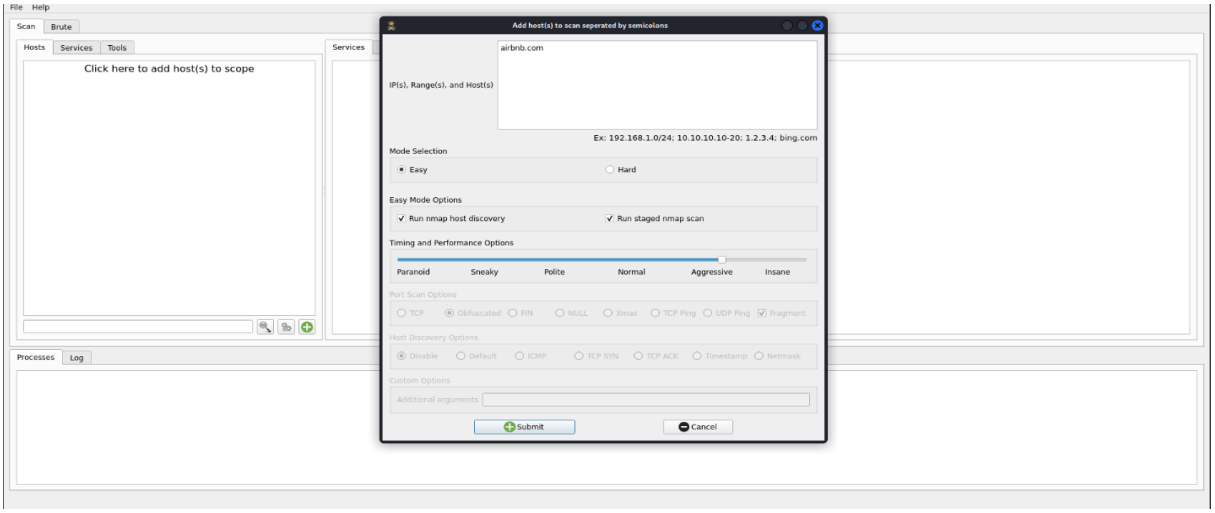
So, I choose that the most suitable vulnerability detection tool according to the gathered information and the usability of those tools. Because some of those tools are not freeware. So, Legion, Nikto, Arachni, Uniscan, Netsparker, Owasp Zap are the tool chosen for use in this Bug Bounty assessment.

➢ Legion

Legion is an open-source network vulnerability detection tool to discover online devices in a network, obtain useful information about targeted systems, and expose targeted system exploits. This tool is a combination of vulnerability detecting tools. Such as Nmap, Whatweb, sslyzer, vulners, SMBenum, and Shodan tools are used in the Legion tool. So, do not need to use Nmap and other tools to detect vulnerabilities in the targeted system.

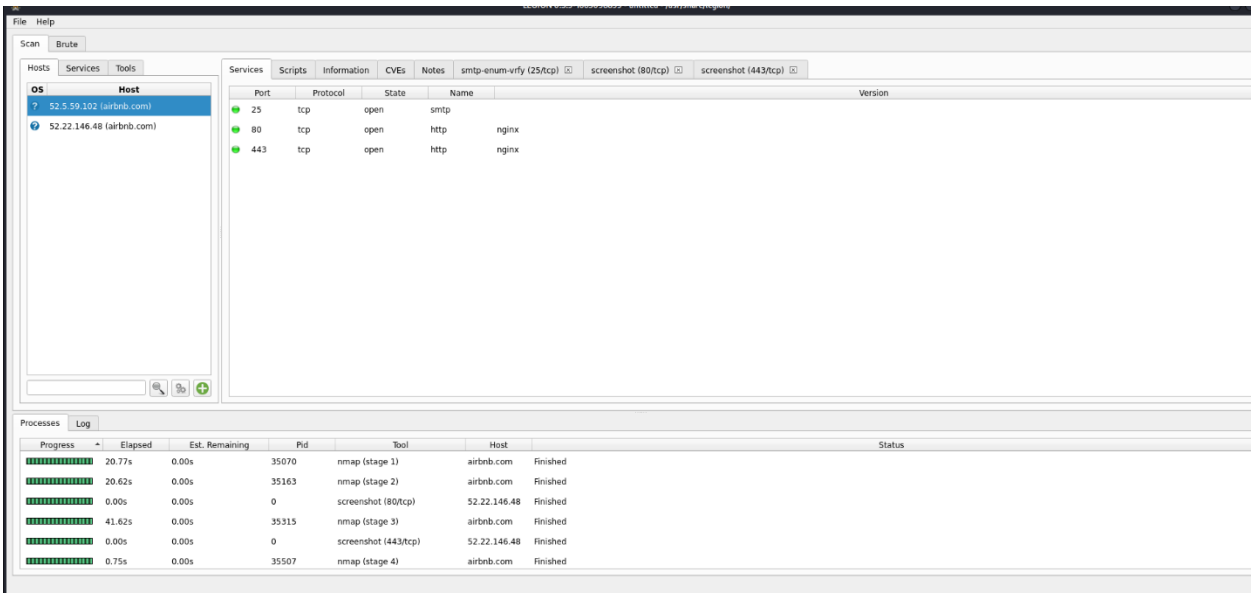


This is the dashboard of the Legion tool. Using the green plus button we can do any type of customization to scan vulnerabilities and provide relevant subdomain links to this tool.



So, I choose automated scan because I need a full scan report of targeted domains and this tool did not take much time to scan. Targeted domain IP address or hostname can use to identify the targeted system and even automated scan this tool provides some Nmap customization methods. After that the customization process is done, we need to submit to get the scanning result from this tool.

Other domains also give almost identical to the main domain result. And port 80 is an open port that is vulnerable to exploitation.

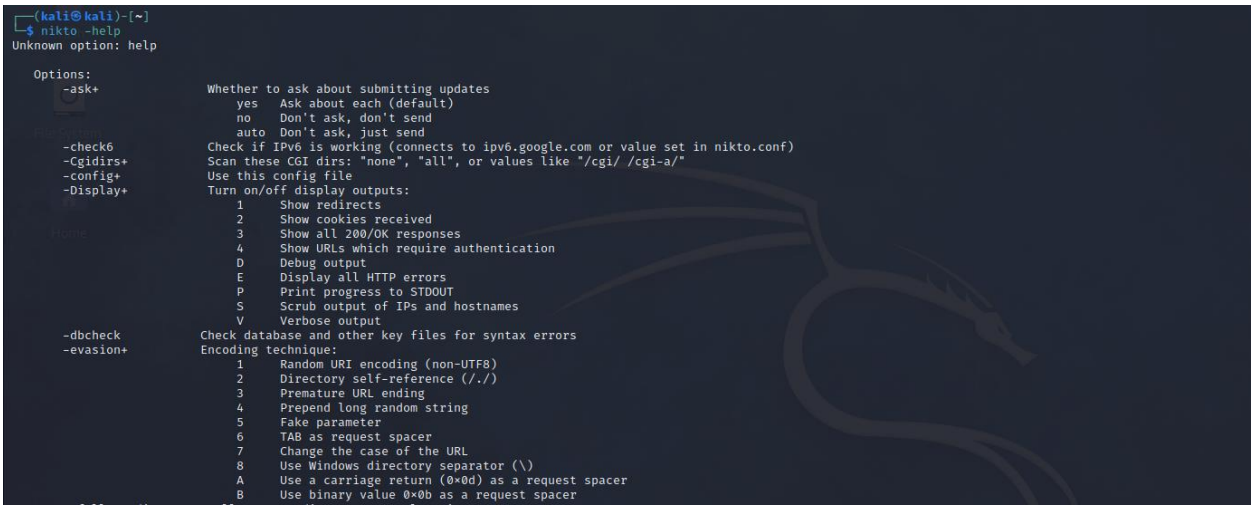


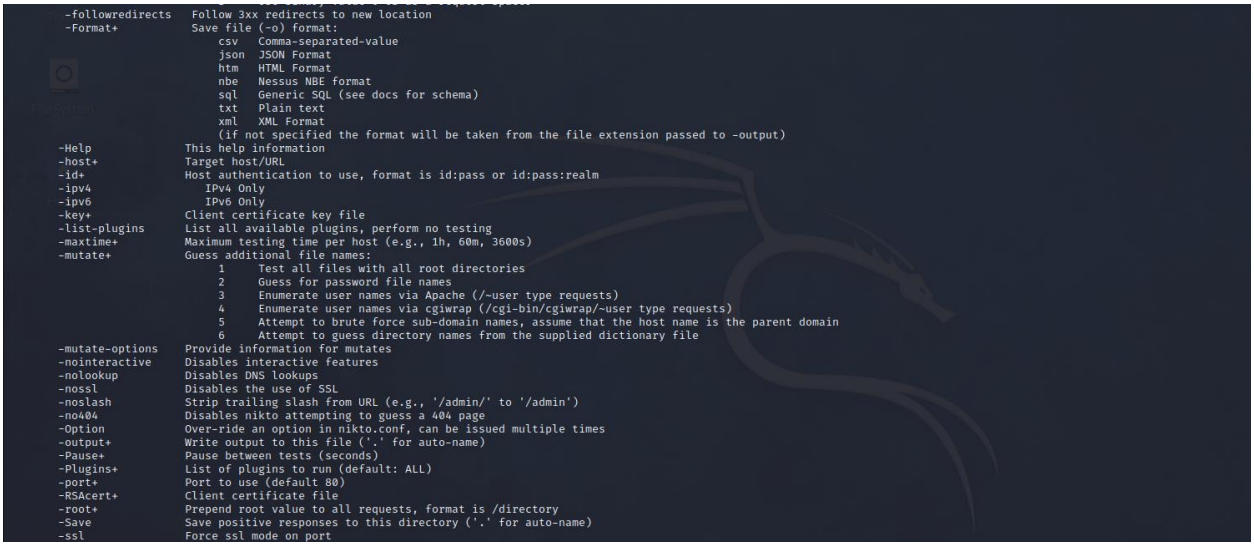
Port scanning also the same result given through the nmap scanning done in the information gathering stage. Because that is the same tool used in this scan. 25 port(SMTP), 80 port(HTTP), 443 port(HTTP) are the open port in the targeted domain. Port 80 can use to exploit vulnerabilities. Because that port is not a protected HTTP port.

➢ Nikto

Nikto is a web vulnerability scanner that use to detect vulnerabilities on the targeted domain server. This tool detects that the server misconfiguration done by the developers. So, the Nikto tool can find misconfiguring ports in the targeted subdomain and output what type of vulnerabilities have in those subdomains.

- To get a better idea about the Nikto tool we can use the “nikto –help” command.





```
-Tuning+          Scan tuning:
                       1     Interesting File / Seen in logs
                       2     Misconfiguration / Default File
                       3     Information Disclosure
                       4     Injection (XSS/Script/HTML)
                       5     Remote File Retrieval - Inside Web Root
                       6     Denial of Service
                       7     Remote File Retrieval - Server Wide
                       8     Command Execution / Remote Shell
                       9     SQL Injection
                       0     File Upload
                       a     Authentication Bypass
                       b     Software Identification
                       c     Remote Source Inclusion
                       d     WebService
                       e     Administrative Console
                       x     Reverse Tuning Options (i.e., include all except specified)
-timeout+         Timeout for requests (default 10 seconds)
-Userdbs          Load only user databases, not the standard databases
                       all   Disable standard dbs and load only user dbs
                       tests Disable only db_tests and load udb_tests
-useragent        Over-rides the default useragent
-until            Run until the specified time or duration
-url+             Target host/URL (alias of -host)
-usecookies       Use cookies from responses in future requests
-useproxy         Use the proxy defined in nikto.conf, or argument http://server:port
-Version          Print plugin and database versions
-vhost+           Virtual host (for Host header)
-404code          Ignore these HTTP codes as negative responses (always). Format is "302,301".
-404string        Ignore this string in response body content as negative response (always). Can be a regular expression.
        + requires a value
```

So, now we need open ports scan details that were collected during the information gathering stage using the Nmap tool to get the scan result of the Nikto tool. According to the Nmap scan results, I scan all open ports use in all the targeted subdomains. So, we can use to input the hostname to the Nikto tool “-h” command and input the port address “-p” command.

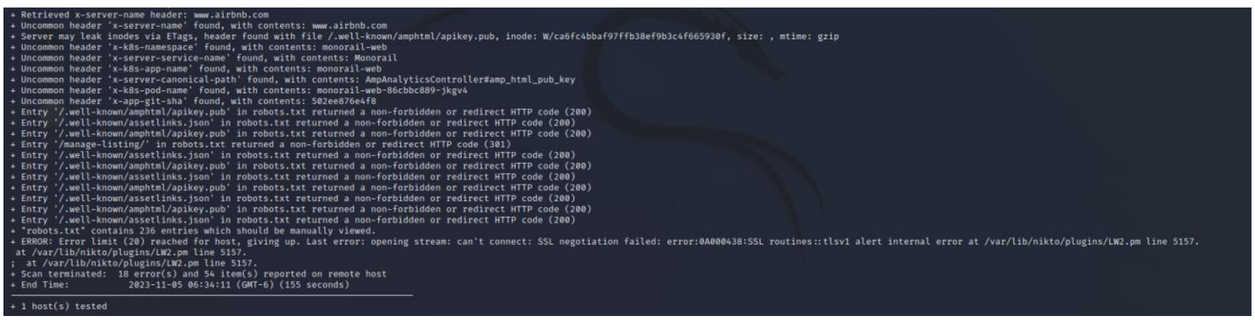
- Scan result of the www.airbnb.com using open port 25

```
┌──(root㉿kali)-[/home/kaveesha]
└─# nikto -h www.airbnb.com -p 25
- Nikto v2.1.6
---------------------------------------------------------------------------
+ No web server found on www.airbnb.com:25
---------------------------------------------------------------------------
+ 0 host(s) tested
```

- Scan result of the www.airbnb.com using open port 25

```
┌──(root㉿kali)-[/home/kaveesha]
└─# nikto -h www.airbnb.com -p 80
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          125.214.166.27
+ Target Hostname:    www.airbnb.com
+ Target Port:        80
+ Message:           Multiple IP addresses found: 125.214.166.27, 125.214.166.25, 125.214.166.26
+ Start Time:        2023-11-05 06:34:56 (GMT-6)
---------------------------------------------------------------------------
+ Server: AkamaiGHost
+ Cookie bev created without the httponly flag
+ Cookie country created without the httponly flag
+ Cookie cdn_exp_c112226c2b200fef6 created without the httponly flag
+ Cookie cdn_exp_5577d10ed9a3b09e4 created without the httponly flag
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'server-timing' found, with contents: cdn-cache; desc=NO-STORE, edge; dur=0, origin; dur=UNSET
+ Uncommon header 'x-erf-bev-bev' found, with contents: 1699187698_N2M3M2Y2MDc2YTk3
+ Uncommon header 'x-erf-bev-bev-is-generated' found, with contents: 1
+ Uncommon header 'x-airbnb-sureride' found, with contents: c1a1r.18.16a6d67d.1699187698.112d94d0%%h1
+ Uncommon header 'x-browser-type' found, with contents: unknown
+ Uncommon header 'cachestatus' found, with contents: on
+ Uncommon header 'origin-trial' found, with contents: AkOekvxwprBL5P7I2nhyRn5yZGt9lTJN6UIYziFKVYgSOhlzmlNDciWbBWkEQ5TYPz+aqsuIUT2pPEjPUD5dFAsAAABneyJvcmlnaW4iOiJodHRwczovL2FpcmJuYi5jb20fNDQzIiwiZmVhdHVyZSI6IlByaW9yaXR5SGludHNBUEkiLCJleHBpcnkiOjE2NDc5OTM1OTksImlzU3ViZG9tYWluIjp0cnVlfQ==
+ Uncommon header 'x-reference-error' found, with contents: 18.16a6d67d.1699187698.112d94d0
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ All CGI directories 'found', use '-C none' to test none
```

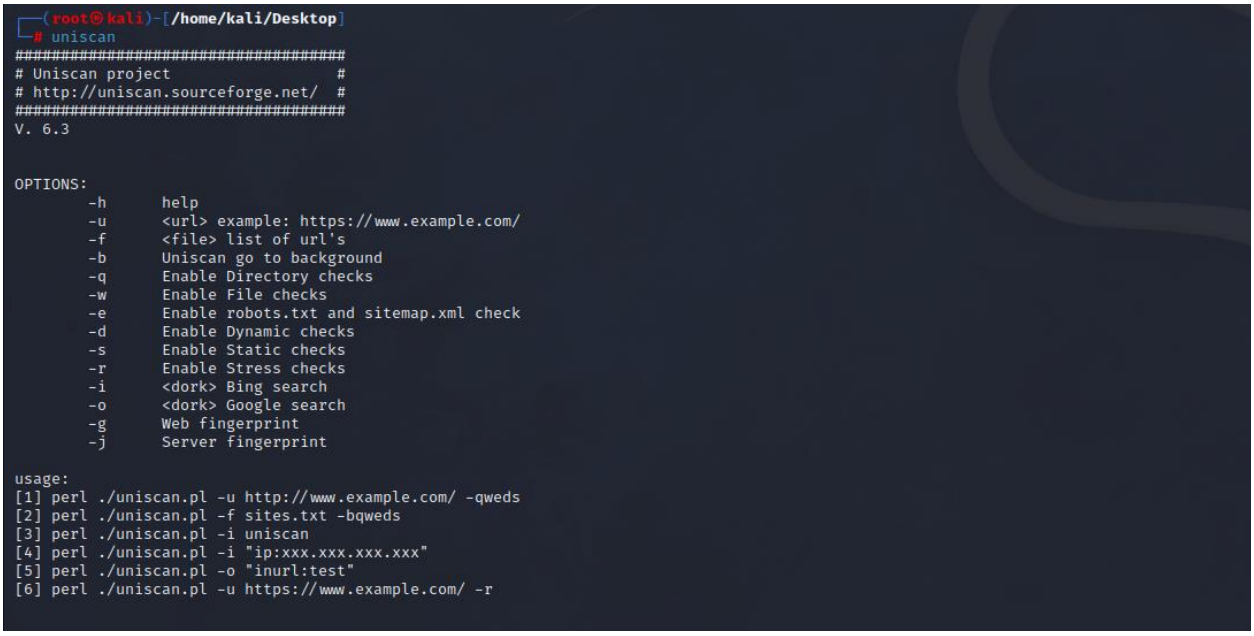
- Scan result of the www.airbnb.com using open port 25



➢ Uniscan

Uniscan is an open-source vulnerability detection tool that can be used to scan vulnerabilities in the targeted web application, such as, cross-site scripting(XSS), remote file inclusion, web shell vulnerabilities, SQL injection, blind SQL injection, and hidden backdoors. Also, the Uniscan tool is capable to do a Bing and Google search for finding domains on shared IP addresses.

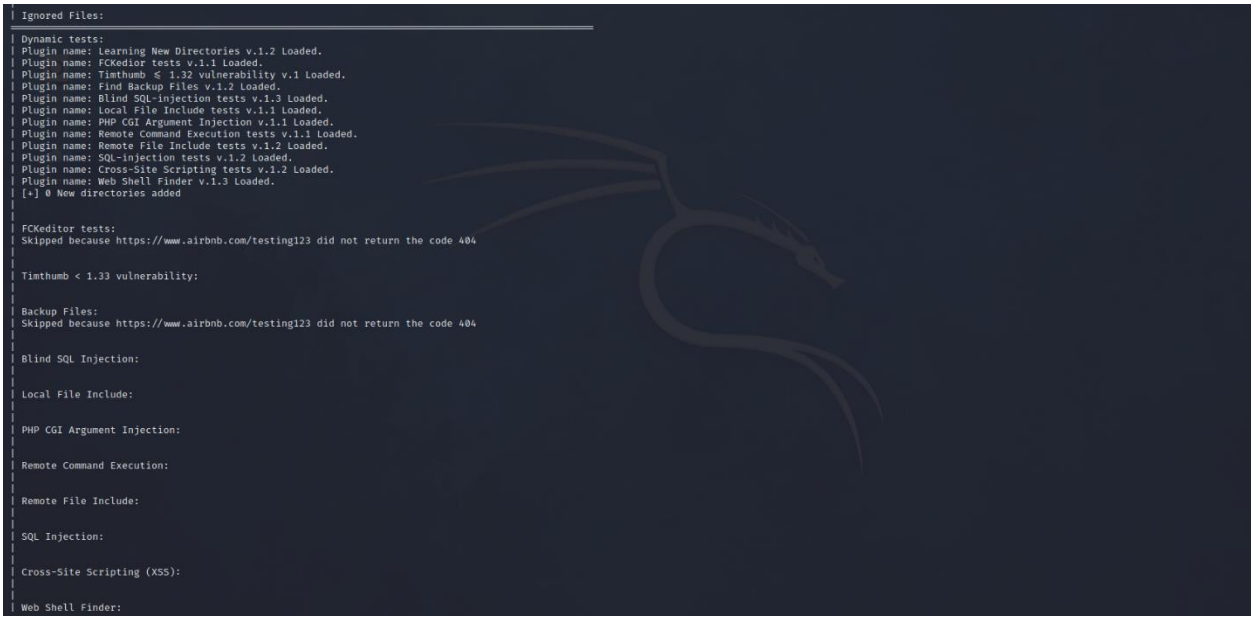
So, this tool is inbuilt in the Kali Linux operating system, and we need to give root permission to access this tool. Uniscan tool can be manually configurable. So, this tool is suitable for the filtered way of scanning.



These are the commands used to filter the scanning results. Because of that the manual configuration efficiently gets the scan result.

```
┌──(root㉿kali)-[/home/kali]
└─# uniscan -u "https://www.airbnb.com/" -j
########################################
# Uniscan project                      #
# http://uniscan.sourceforge.net/  #
########################################
V. 6.3


Scan date: 5-11-2023 8:4:46
============================================================================
| Domain: https://www.airbnb.com/
Use of uninitialized value in unpack at /usr/share/uniscan/Uniscan/Functions.pm line 62.
| IP:
Use of uninitialized value in unpack at /usr/share/uniscan/Uniscan/Functions.pm line 62.
============================================================================
| PING
|
ping: www.airbnb.com: Temporary failure in name resolution
============================================================================
| TRACEROUTE
|
www.airbnb.com: Temporary failure in name resolution
Cannot handle "host" cmdline arg `www.airbnb.com' on position 1 (argc 1)
============================================================================
| NSLOOKUP
|
| ;; communications error to ::1#53: connection refused
| ;; communications error to 127.0.0.1#53: connection refused
| ;; no servers could be reached
|
| ;; Connection to ::1#53(::1) for www.airbnb.com failed: connection refused.
| ;; Connection to 127.0.0.1#53(127.0.0.1) for www.airbnb.com failed: connection refused.
============================================================================
| NMAP
|
Failed to resolve "www.airbnb.com".
WARNING: No targets were specified, so 0 hosts scanned.
| Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-05 08:04 EST
| NSE: Loaded 156 scripts for scanning.
| NSE: Script Pre-scanning.
| Initiating NSE at 08:04
| Completed NSE at 08:04, 0.00s elapsed
| Initiating NSE at 08:04
| Completed NSE at 08:04, 0.00s elapsed
| Initiating NSE at 08:04
| Completed NSE at 08:04, 0.00s elapsed
| NSE: Script Post-scanning.
| Initiating NSE at 08:04
| Completed NSE at 08:04, 0.00s elapsed
| Initiating NSE at 08:04
| Completed NSE at 08:04, 0.00s elapsed
| Initiating NSE at 08:04
| Completed NSE at 08:04, 0.00s elapsed
| Read data files from: /usr/bin/../share/nmap
| Nmap done: 0 IP addresses (0 hosts up) scanned in 0.25 seconds
|           Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
============================================================================
Scan end date: 5-11-2023 8:4:47


HTML report saved in: report/www.airbnb.com.html
```

```
┌──(root㉿kali)-[/home/kali]
└─# uniscan -u "https://www.airbnb.com/" -d
########################################
# Uniscan project                      #
# http://uniscan.sourceforge.net/  #
########################################
V. 6.3


Scan date: 5-11-2023 8:9:32
============================================================================
| Domain: https://www.airbnb.com/
Use of uninitialized value in unpack at /usr/share/uniscan/Uniscan/Functions.pm line 62.
| IP:
Use of uninitialized value in unpack at /usr/share/uniscan/Uniscan/Functions.pm line 62.
============================================================================
|
| Crawler Started:
| Plugin name: External Host Detect v.1.2 Loaded.
| Plugin name: Timthumb ⩽ 1.32 vulnerability v.1 Loaded.
| Plugin name: FCKeditor upload test v.1 Loaded.
| Plugin name: phpinfo() Disclosure v.1 Loaded.
| Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
| Plugin name: Upload Form Detect v.1.1 Loaded.
| Plugin name: Code Disclosure v.1.1 Loaded.
| Plugin name: E-mail Detection v.1.1 Loaded.
| [+] Crawling finished, 1 URL's found!
|
| External hosts:
|
| Timthumb:
|
| FCKeditor File Upload:
|
| PHPinfo() Disclosure:
|
| Web Backdoors:
|
| File Upload Forms:
|
| Source Code Disclosure:
|
| E-mails:
```



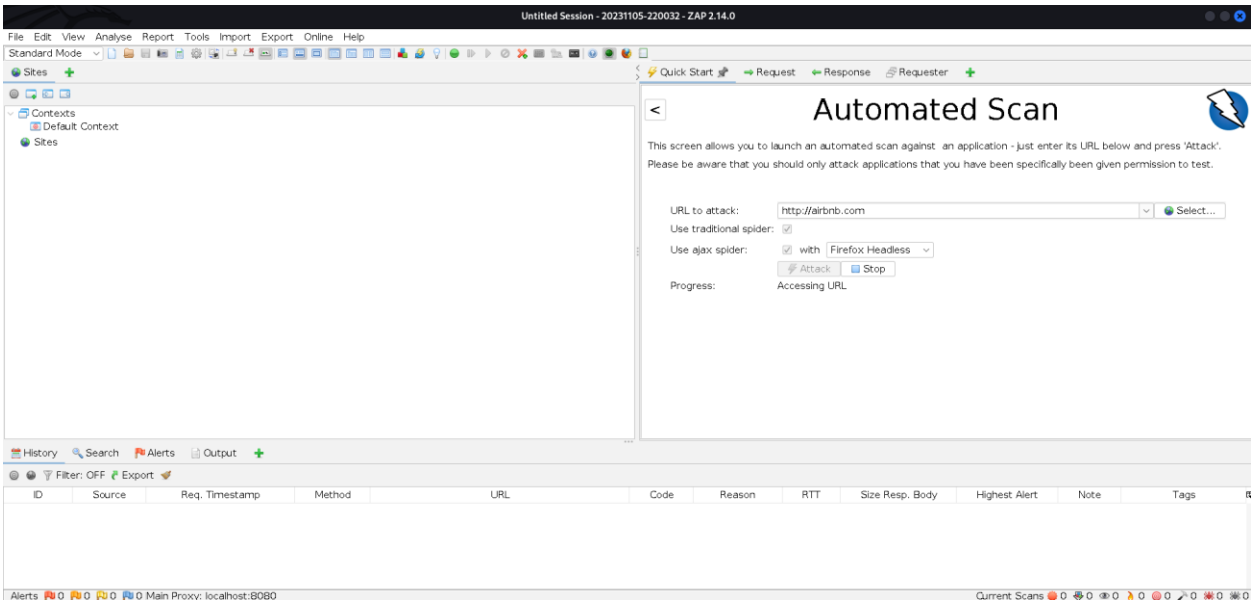
this is the scan result we can get from this tool. So, there are no vulnerabilities captured by this tool. But Nmap and other scan results are important to find vulnerabilities in the targeted system.

➢ Owasp ZAP

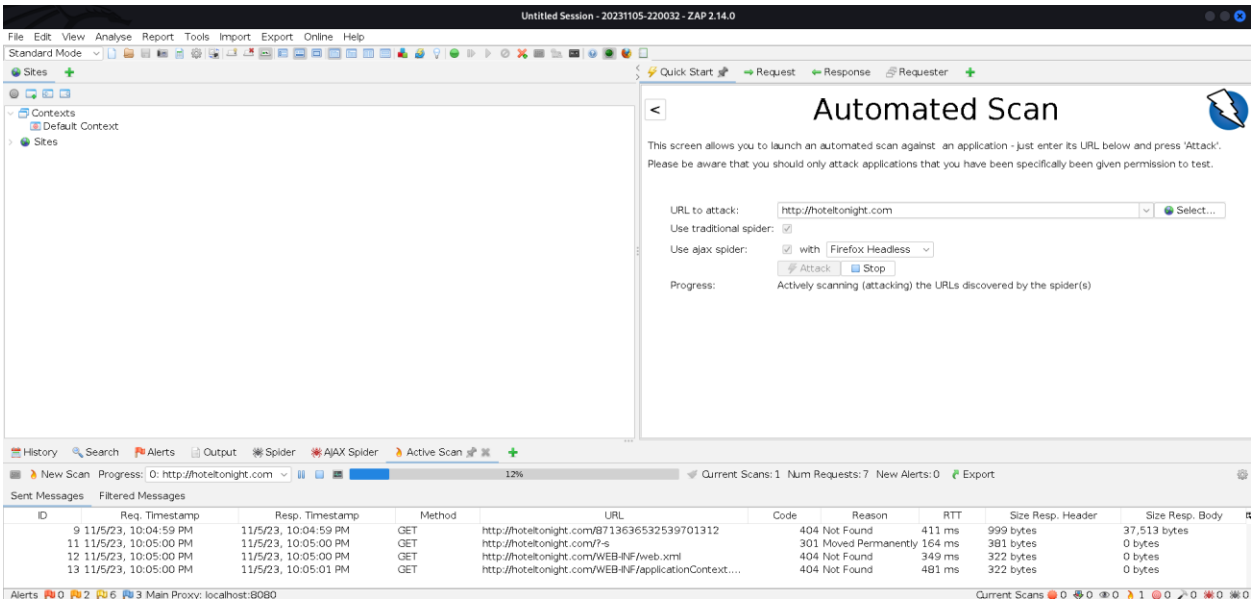
The Open Web Application Security Project Zed Attack Proxy (OWASP ZAP) is an open-source web application vulnerability detection tool. This is one of the best vulnerability detection tools and efficient than compared with most other tools. Owasp ZAP is also can be used as web application professional penetration testers. This tool work according to the OWASP top 10 security threats. Such as Cross-site scripting (XSS), Broken access control, SQL injection, Broken authentication and session management, Security misconfiguration and other security threats.

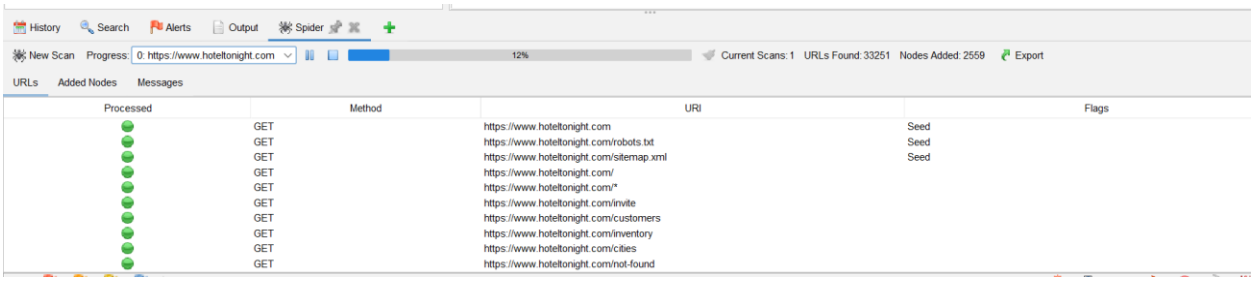
Consider that how does Owasp ZAP work, according to Srijan's Framework and Libraries, "ZAP creates a proxy server and makes your website traffic pass through that server. It comprises of auto scanners that help you intercept the vulnerabilities in your website.". There is an automated or manual scanning option and for this assignment choose that the automated scan method because the automated method filter and scan only the in-scope subdomains. The automated scan is also customizable and if it is customized well, we can reduce that time taken for scanning the targeted subdomain.

- Settle to scan Airbnb.com



- Scanning process of www.hoteltonight.com





Penetration testing

Penetration Testing is an important stage in Bug Bounty Assessment. Because in this stage test the scanned vulnerabilities found in the targeted subdomain. So, we can find out that vulnerabilities are actually exploitable or not. According to the National Institute of Standards and Technology (NIST), “Penetration Testing is a method of testing where testers target individual binary components or the application as a whole to determine whether intra or intercomponent vulnerabilities can be exploited to compromise the application, its data, or its environment resources.”. Also, this process is named ethical hacking or pen-testing. So, this process can help to confirm the vulnerabilities in the targeted system.

Penetration testing is a crucial aspect in the confirmation of data security in every aspect of the data is used today. The necessity of it is highlighted due to the benefits it gives. Penetration tests allow us to identify new bugs and loopholes in existing software, test new software for existing bugs, and whether the implemented security controls are sufficient to handle the latest security threats. It enables us or our company to be able to stay up to standard with recognized international standards like General Data Protection Regulation (EU GDPR), Data Protection Act (DPA), Payment Card Industry Data Security Standard (PSI DSS), fix the identified bugs and loopholes in security controls that have already been implemented to assure our clients and stakeholders that their data is secure.

After confirming those vulnerabilities, we need to report these vulnerabilities and the protection methods to the relevant company belong the targeted system. And this process needs to be done before attackers exploit the system.

Conclusion

The purpose of this assignment was to assess the vulnerabilities of the web application. While engaging in this assignment I was able to identify a lot of Bug Bounty hunting platforms which helped to improve vulnerability assessing skills and knowledge about the penetration testing tool and how to use those tools. I decided to use the Hackerone platform because this website legally protects us to do Bug Bounty hunting for real-world web applications. So I select www.airbnb.com site in my bug bounty program. The web audit reports give an excellent understanding of how to handle cybersecurity professional skills.

References

- Sucuri Guides' Coporate Auther, "Sucuri," 2021. [Online]. Available: https://sucuri.net/guides/owasp top-10-security-vulnerabilities-2021/. [Accessed 11 10 2021].

- AAT TEAM, "All About Teating(AAT)," 21 9 2021. [Online]. Available: https://allabouttesting.org/information-gathering-techniques-for-penetration-testing/. [Accessed 13 10 2021].

- Github, "Sublist3r," Github, 29 6 2020. [Online]. Available: https://github.com/aboul3la/Sublist3r. [Accessed 13 10 2021].

- Kali linux, "WhatWeb," Kali Linux, [Online]. Available: https://www.kali.org/tools/whatweb/. [Accessed 14 10 2021].

- OWASP, "OWASP Cheat Sheet Series," OWASP, 2021. [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html#defending-with-x-frame-options-response-headers. [Accessed 15 10 2021].

- MDN contributors, "MDN Web Docs," Mozilla, 13 7 2021. [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection. [Accessed 15 10 2021].

- Balbix Corporation, "Balbix," Balbix Corporation, 2020. [Online]. Available: https://www.balbix.com/insights/what-is-vulnerability-scanning/. [Accessed 17 10 2021].

- MDN contributors, "MDN Web Docs," Mozilla, 4 10 2021. [Online]. Available: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options. [Accessed 24 10 2021].

- Netsparker Corporate, "What is Netsparker?," Netsparker, 2021. [Online]. Available: https://www.netsparker.com/support/what-is-netsparker/. [Accessed 27 10 2021].

- Edpresso Team, "What is Lodash?," Educative, [Online]. Available: https://www.educative.io/edpresso/what-is-lodash. [Accessed 25 10 2021]