Lab#1 Active and Passive Reconn

Tool	Type	Platform	Use	How to Use
The Harvester	Passive	Linux, Windows, macOS	Harvests information from various sources	Harvests emails, subdomains, hosts, and employee names
Maltego	Passive	Linux, Windows, macOS	Visualizes and analyzes data relationships	Maps relationships between individuals and organizations
Spider Foot	Passive	Linux, Windows, macOS	Gathers information from different sources	Collects data from public sources and performs analysis
Shodan	Passive	Web	Searches for devices and services on the Internet	Finds devices, banners, and vulnerabilities
ZoomEye.org	Passive	Web	Searches for Internet-connected devices and services	Identifies open ports and services
Censys.io	Passive	Web	Collects data on hosts and websites	Scans for network information and vulnerabilities
Spyse.com	Passive	Web	Collects data on IP addresses, domains, and technologies	Gathers information about assets and technologies
OSINT Framework	Passive	Linux, Windows, macOS	Aggregates various OSINT tools and resources	Accesses multiple OSINT tools through a unified interface
FOCA	Passive	Windows	Metadata analysis in documents	Extracts metadata from documents
Have I Been Pwned	Passive	Web	Checks if email addresses have been part of data breaches	Searches for email addresses in data breach databases
Amass	Active	Linux, Windows, macOS	Subdomain enumeration and network mapping	Enumerates subdomains and discovers network infrastructure
Sn1per	Active	Linux, Windows	Automated reconnaissance and vulnerability scanning	Scans for vulnerabilities and potential entry points
Recon-NG	Active	Linux	Full-featured web reconnaissance framework	Gathers information about web applications and domains
SET (Social Engineering Toolkit)	Active	Linux	Social engineering attacks and credential harvesting	Creates and launches social engineering campaigns
Nikto	Active	Linux, Windows	Web server vulnerability scanner	Identifies vulnerabilities in web servers
Sublist3r	Active	Linux, Windows, macOS	Subdomain enumeration tool	Enumerates subdomains from different sources
Nmap	Active	Linux, Windows, macOS	Network scanning and mapping	Scans networks for open ports and services
Metasploit Framework	Active	Linux, Windows, macOS	Vulnerability exploitation tool	Develops, tests, and executes exploit code
SQLmap	Active	Linux, Windows, macOS	Automated SQL injection and database takeover tool	Exploits SQL injection vulnerabilities in web applications
Burp Suite	Active	Linux, Windows, macOS	Web vulnerability scanner and penetration testing tool	Identifies vulnerabilities and performs security testing on web applications

Part A: Active Reconnaissance with Reconnaissance Tools

Amass:

Analysis:

I run "amass enum" command on the domain "meesho.com" to gather information about its DNS records, IP addresses, netblocks, and related Autonomous System Numbers (ASNs).

Here's a summary of the information I've obtained:

Domain Information:

- The domain "meesho.com" has various DNS records, including A, AAAA, CNAME, and MX records.
- It uses Cloudflare for content delivery (CDN) for several other sub-domains.
- It has multiple IP addresses associated with it.

Name Servers:

"meesho.com" uses Amazon AWS for its DNS hosting with name servers provided by AWS.

IP Addresses:

- The domain "meesho.com" resolves to multiple IP addresses, including 54.251.178.150, 52.77.54.140,

52.76.137.43, and more.

- Several other subdomains also have associated IP addresses.

Netblocks:

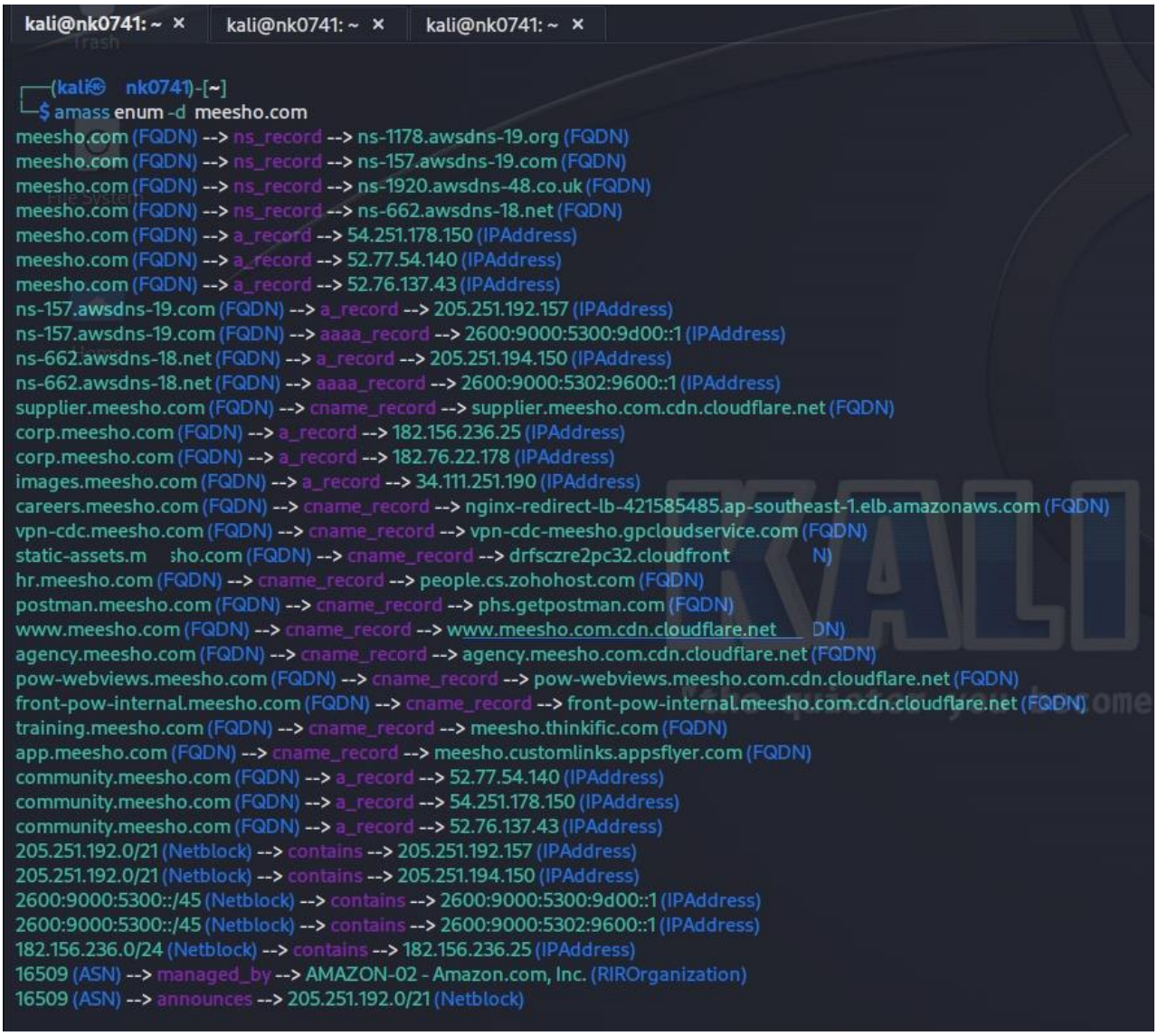
- Several netblocks are associated with the IP addresses used by "meesho.com,"

Some of them are: 205.251.192.0/21, 2600:9000:5300::/45, and others.

Autonomous System Numbers (ASNs):

- AS16509 (Amazon.com, Inc.) manages some of the IP addresses used by "meesho.com."
- AS45820 (Tata Teleservices ISP AS, IN) manages other IP addresses.
- AS14618 (Amazon.com, Inc.) and AS9498 (BHARTI Airtel Ltd., IN) also manage certain IP blocks.
- AS13335 (Cloudflare, Inc.) is involved in providing CDN services.
- AS15169 (Google LLC) and AS243 (Harris Government Systems Sector) are associated with some IP blocks.

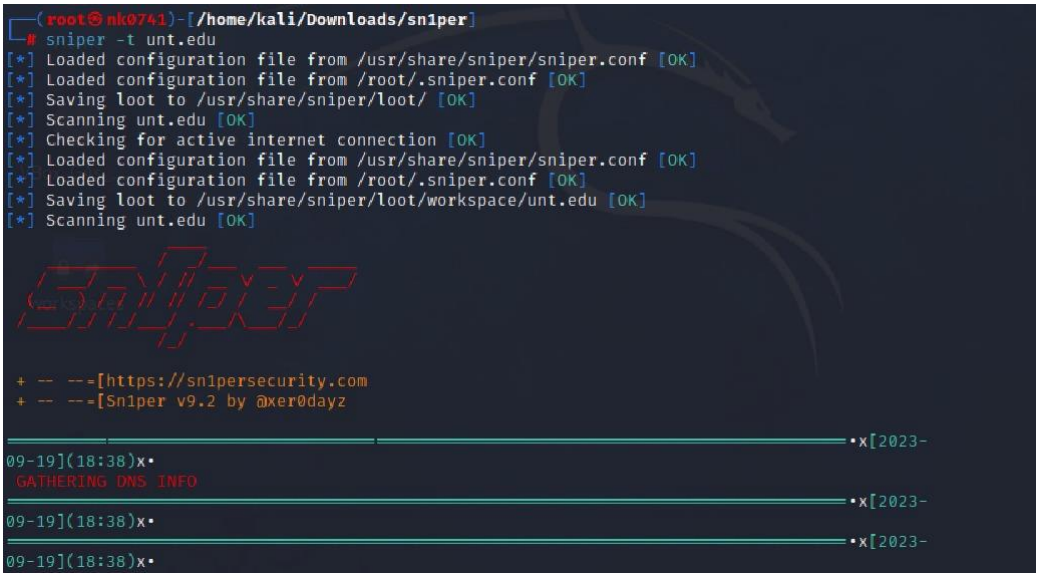
This information can be useful for network analysis, security, and understanding the infrastructure of the "meesho.com" domain.

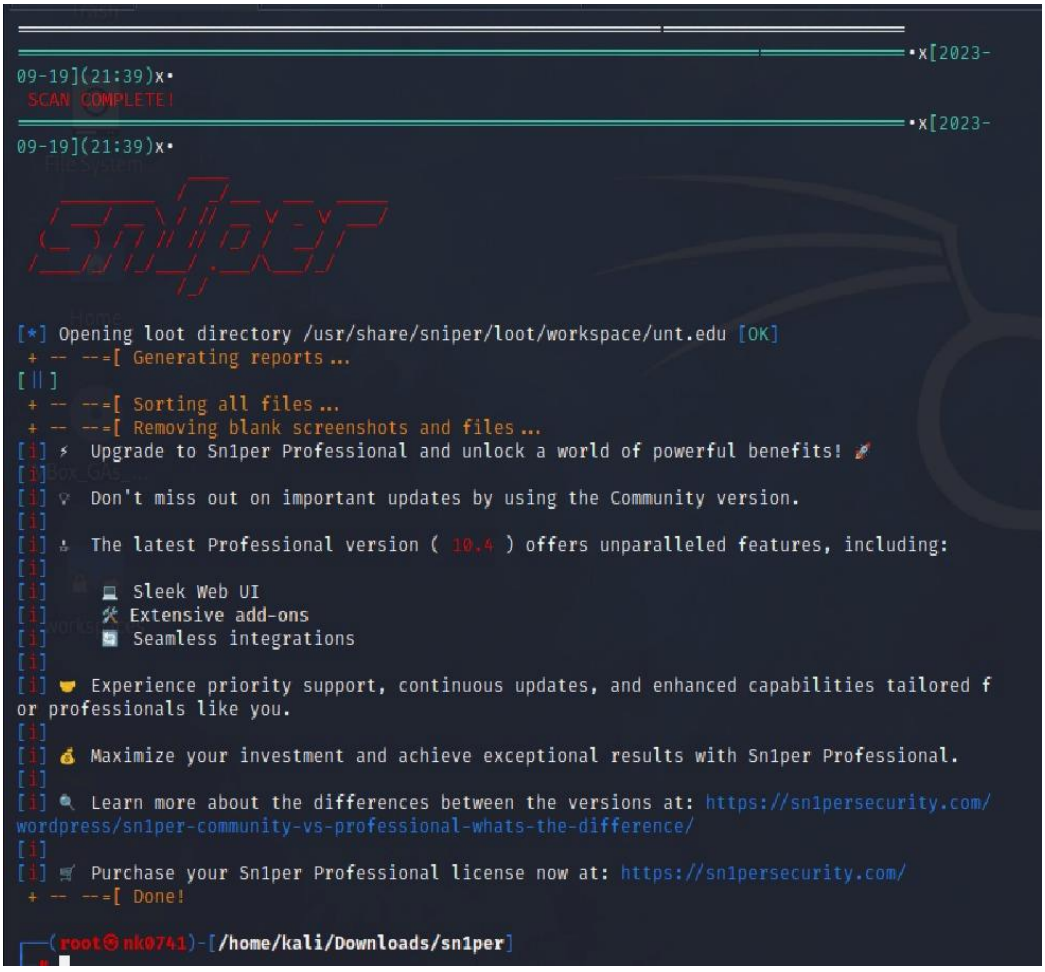


```
front-pow-internal.meesho.com.cdn.cloudflare.net (FQDN) --> a_record --> 172.64.149.243 (IPAddress)
front-pow-internal.meesho.com.cdn.cloudflare.net (FQDN) --> a_record --> 104.18.38.13 (IPAddress)
front-pow-internal.meesho.com.cdn.cloudflare.net (FQDN) --> aaaa_record --> 2606:4700:4400::6812:260d (IPAddress)
front-pow-internal.meesho.com.cdn.cloudflare.net (FQDN) --> aaaa_record --> 2606:4700:4400::ac40:95f3 (IPAddress)
alt1.aspmx.l.google.com (FQDN) --> a_record --> 172.253.113.26 (IPAddress)
alt1.aspmx.l.google.com (FQDN) --> aaaa_record --> 2607:f8b0:4023:1::1b (IPAddress)
108.156.240.0/21 (Netblock) --> contains --> 108.156.245.35 (IPAddress)
108.156.240.0/21 (Netblock) --> contains --> 108.156.245.73 (IPAddress)
108.156.240.0/21 (Netblock) --> contains --> 108.156.245.59 (IPAddress)
2600:9000:2341::/48 (Netblock) --> contains --> 2600:9000:2341:e400:8:7bec:db80:93a1 (IPAddress)
2600:9000:2341::/48 (Netblock) --> contains --> 2600:9000:2341:2a00:8:7bec:db80:93a1 (IPAddress)
2600:9000:2341::/48 (Netblock) --> contains --> 2600:9000:2341:dc00:8:7bec:db80:93a1 (IPAddress)
2600:9000:2341::/48 (Netblock) --> contains --> 2600:9000:2341:b600:8:7bec:db80:93a1 (IPAddress)
2607:f8b0::/32 (Netblock) --> contains --> 2607:f8b0:4023:400::1b (IPAddress)
2607:f8b0::/32 (Netblock) --> contains --> 2607:f8b0:4003:c10::1a (IPAddress)
172.253.126.0/24 (Netblock) --> contains --> 172.253.126.27 (IPAddress)
172.253.126.0/24 (Netblock) --> contains --> 172.253.126.26 (IPAddress)
34.108.0.0/14 (Netblock) --> contains --> 34.111.251.190 (IPAddress)
54.166.0.0/15 (Netblock) --> contains --> 54.166.217.23 (IPAddress)
52.77.0.0/16 (Netblock) --> contains --> 52.77.54.140 (IPAddress)
54.251.160.0/19 (Netblock) --> contains --> 54.251.178.150 (IPAddress)
16509 (ASN) --> announces --> 52.77.0.0/16 (Netblock)
16509 (ASN) --> announces --> 54.251.160.0/19 (Netblock)
14618 (ASN) --> announces --> 54.166.0.0/15 (Netblock)
15169 (ASN) --> announces --> 172.253.126.0/24 (Netblock)
396982 (ASN) --> managed_by --> GOOGLE-CLOUD-PLATFORM, US (RIROrganization)
396982 (ASN) --> announces --> 34.108.0.0/14 (Netblock)
supplier.meesho.com.cdn.cloudflare.net (FQDN) --> a_record --> 104.18.38.13 (IPAddress)
supplier.meesho.com.cdn.cloudflare.net (FQDN) --> a_record --> 172.64.149.243 (IPAddress)
supplier.meesho.com.cdn.cloudflare.net (FQDN) --> aaaa_record --> 2606:4700:4400::6812:260d (IPAddress)
supplier.meesho.com.cdn.cloudflare.net (FQDN) --> aaaa_record --> 2606:4700:4400::ac40:95f3 (IPAddress)
nginx-redirect-lb-421585485.ap-southeast-1.elb.amazonaws.com (FQDN) --> a_record --> 52.220.245.111 (IPAddress)
nginx-redirect-lb-421585485.ap-southeast-1.elb.amazonaws.com (FQDN) --> a_record --> 3.0.164.162 (IPAddress)
nginx-redirect-lb-421585485.ap-southeast-1.elb.amazonaws.com (FQDN) --> a_record --> 52.220.242.60 (IPAddress)

The enumeration has finished

┌──(kali㉿ nk0741)-[~]
```

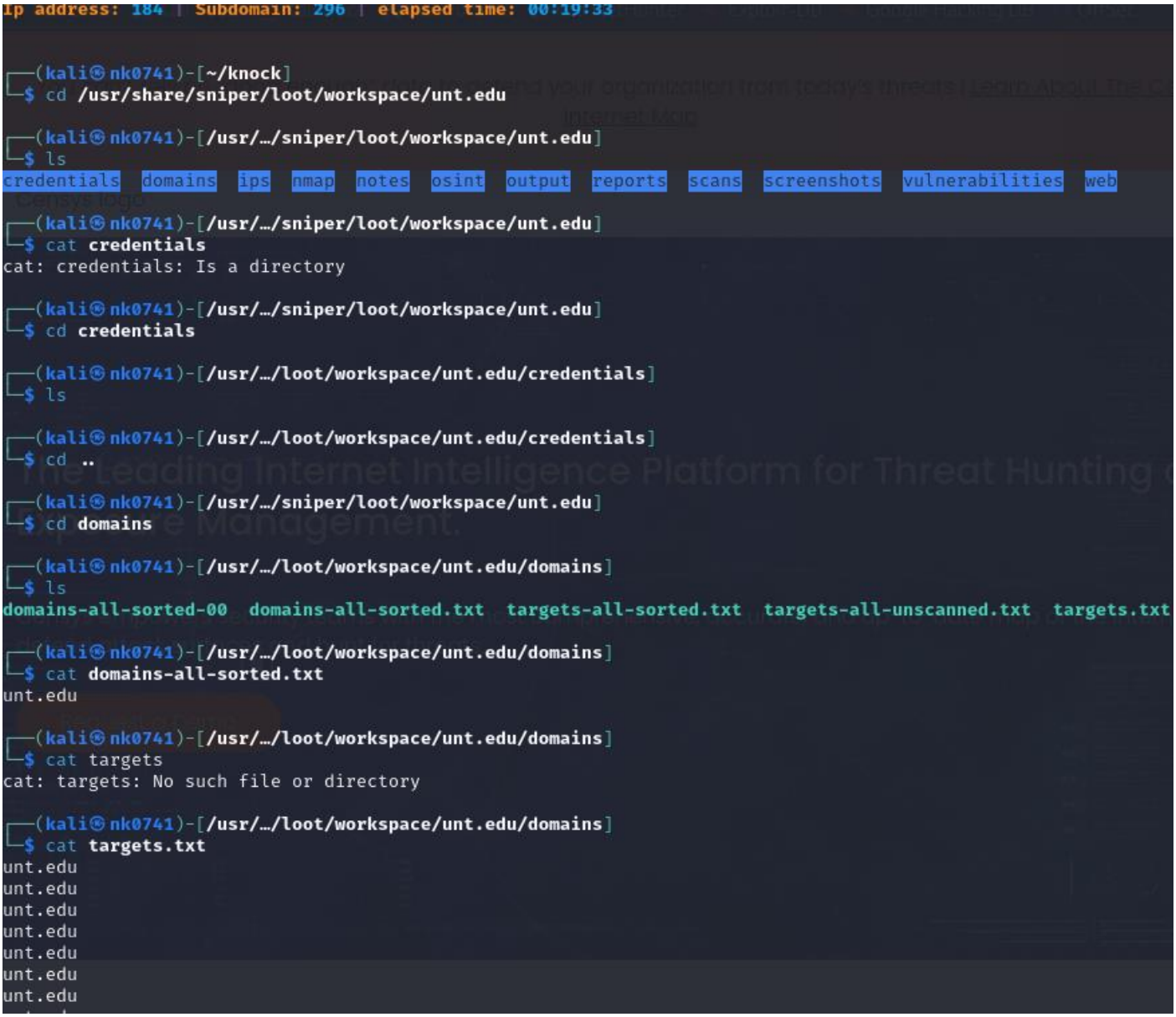
Sn1per: Sn1per is an automated tool that combines various open-source tools and scanning techniques to assist in reconnaissance and vulnerability assessment. It streamlines the information-gathering process and automates the scanning of targets to identify potential vulnerabilities.

```
┌──(root㉿nk0741)-[/home/kali/Downloads/sn1per]
└─# bash install.sh

 + -- --=[ https://sn1persecurity.com
 + -- --=[ Sn1per CE by @xer0dayz

[>] This script will install Sn1per under /usr/share/sniper. Are you sure you want to contin
ue? (Hit Ctrl+C to exit)

[*] Installing package dependencies...
Hit:1 http://mirrors.jevincanders.net/kali kali-rolling InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
532 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
python3-paramiko is already the newest version (2.12.0-2).
python3-paramiko set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 532 not upgraded.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nfs-common is already the newest version (1:2.6.3-3).
nfs-common set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 532 not upgraded.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```





It can do the following activities: Automated Scanning
Customization
Integration of Tools
Report Generation
Port Scanning
Vulnerability Scanning
Below is the screenshot showing the results of the using sn1per and list of files in it.



SET (Social Engineering Toolkit):

Analysis:

After trying to use the SET multiples times, below is the explanation for two of them and steps I followed to perform it.

Step 1: Choosing an Attack Vector

I chose the "Website Attack Vectors" option which is used to create web-based attacks.

Step 2: Choosing a Web Attack Method

In this step I selected the "Metasploit Browser Exploit Method" and "Java Applet Attack Method" in different instances.
Both methods are designed to exploit vulnerabilities in the web browser or Java runtime of the victim's machine.
The Metasploit method utilizes selected Metasploit browser exploits through an iframe to deliver a payload,
While the Java Applet method uses a malicious Java applet to deliver the payload.

Step 3: Cloning a Website

I chose to clone a website (gmail.com) to create a malicious copy of the site.
This cloned site will host the malicious payload.

Step 4: Configuring Network Settings

It prompted to configure network settings, including whether NAT/Port Forwarding is being used and the IP address of the SET web server.

Step 5: Configuring Payload

It prompted to choose a payload for the attack. In different instances, you chose different payloads:

1. In the first instance (Metasploit Browser Exploit Method), you selected a shellcode payload targeting Mozilla Firefox.
2. In the second instance (Java Applet Attack Method), you chose the SET Interactive Shell, which is a custom reverse shell developed for SET.

Step 6: Launching the Attack

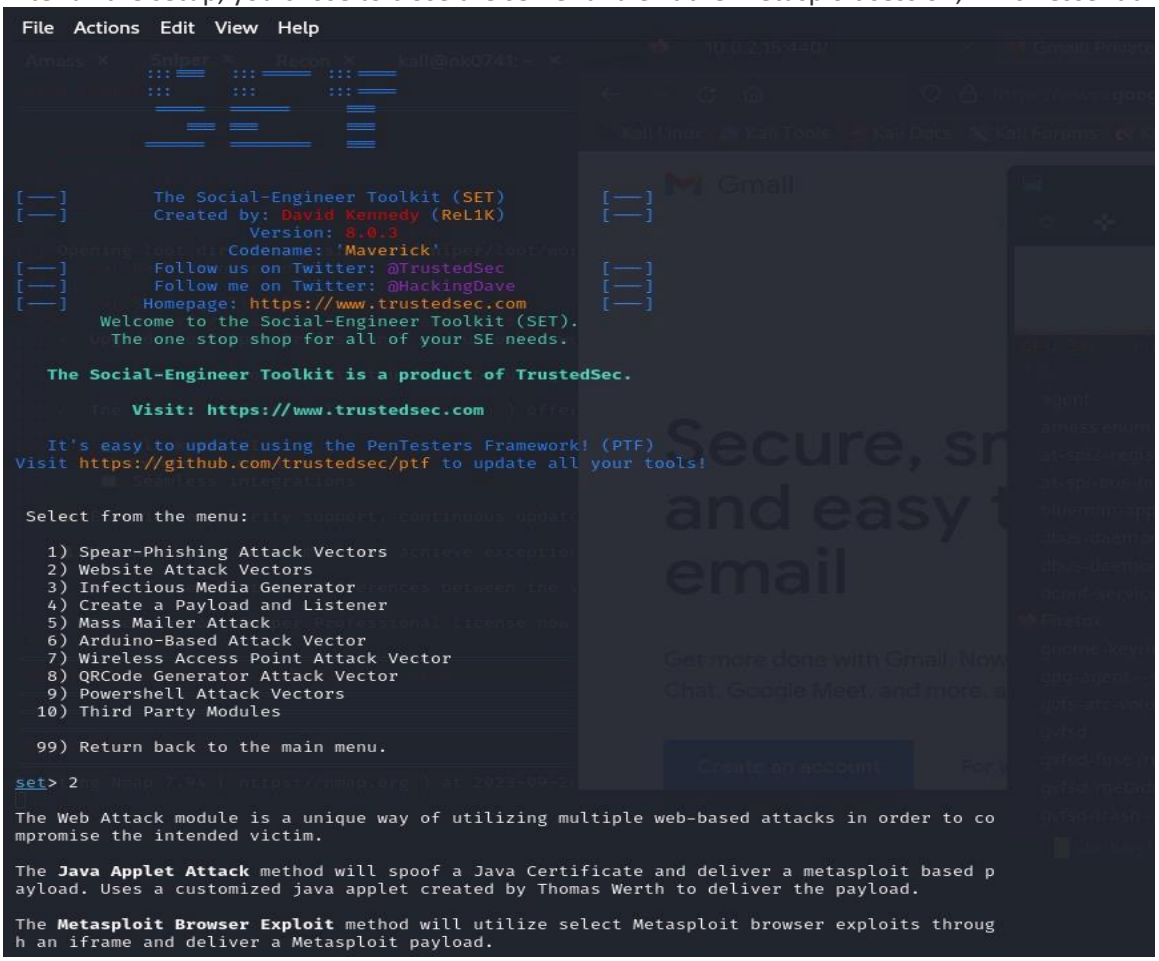
After configuring the settings, SET started a web server to host the malicious website (clone of gmail.com) with the injected payload. It seems the server started successfully, and it's ready to serve the malicious website to potential victims.

Step 7: Starting the Metasploit Framework

SET also initialized the Metasploit Framework to handle the connections from the victims when they interact with the malicious website.

Step 8: Closure

After all the setup, you chose to close the server and exit the Metasploit session, which essentially stopped the attack.



```
File  Actions  Edit  View  Help
What payload do you want to generate:

  Name:                                  Description:

   1) Meterpreter Memory Injection (DEFAULT)  This will drop a meterpreter payload through powershell injection
   2) Meterpreter Multi-Memory Injection      This will drop multiple Metasploit payloads via powershell injection
   3) SE Toolkit Interactive Shell            Custom interactive reverse toolkit designed for SET
   4) SE Toolkit HTTP Reverse Shell           Purely native HTTP shell with AES encryption support
   5) RATTE HTTP Tunneling Payload            Security bypass payload that will tunnel all comms over HTTP
   6) ShellCodeExec Alphanum Shellcode        This will drop a meterpreter payload through shellcodeexec
   7) Import your own executable              Specify a path for your own executable
   8) Import your own commands.txt            Specify payloads to be sent via command line

set:payloads>3

*************************************************
Web Server Launched. Welcome to the SET Web Attack.
*************************************************

[--] Tested on Windows, Linux, and OSX [--]
[*] Moving payload into cloned website.
[*] The site has been moved. SET Web Server is now listening..
Press <return> when you want to shut down the web server. It is currently listening.


[-] Launching the SET Interactive Shell...
127.0.0.1 - - [20/Sep/2023 01:08:07] "QUIT / HTTP/1.1" 200 -

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deli

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the webs

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitima
s link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credentia

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitati

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu
```

Recon-ng:

```
[*] Version check disabled.

    Sponsored by ...
                                  www.blackhillsinfosec.com

                                  www.practisec.com

                    [recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[85] Recon modules
[13] Disabled modules
[8]  Reporting modules
[4]  Import modules
[2]  Exploitation modules
[2]  Discovery modules

[recon-ng][default] > workspaces create nk0741
[!] 'shodan_api' key not set. shodan_org module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_miner module will likely fail at runtime. See 'keys add'.
[!] Module 'recon/domains-contacts/metacrawler' disabled. Dependency required: ''PyPDF3''.
```

Opening Recon-ng and creating the workspace: nk0741

```
  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.

[recon-ng][nk0741] > marketplace search ssl
[*] Searching module index for 'ssl' ...

  +-------------------------------------------------------------------------+
  |             Path             | Version |   Status  |  Updated   | D | K |
  +-------------------------------------------------------------------------+
  | recon/domains-hosts/ssl_san  | 1.0     | installed | 2019-06-24 |   |   |
  | recon/hosts-hosts/ssltools   | 1.0     | installed | 2019-06-24 |   |   |
  | recon/ports-hosts/ssl_scan   | 1.1     | installed | 2021-08-24 |   |   |
  +-------------------------------------------------------------------------+

  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.

[recon-ng][nk0741] > marketplace install hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules ...
[!] 'shodan_api' key not set. shodan_org module will likely fail at runtime. See 'keys add'.
[!] 'github_api' key not set. github_miner module will likely fail at runtime. See 'keys add'.
```

Using marketplace to search for ssl module and installing it.

```
[!] 'censys.search' (/usr/local/lib/python3.11/dist-packages/censys/search/__init__.py).
[!] 'google_api' key not set. pushpin module will likely fail at runtime. See 'keys add'.
[recon-ng][nk0741] > modules load hackertarget
[recon-ng][nk0741][hackertarget] > show options
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|reposit
ories|vulnerabilities>

[recon-ng][nk0741][hackertarget] > options set SOURCE tesla.com
SOURCE => tesla.com
[recon-ng][nk0741][hackertarget] > info

      Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
   Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  tesla.com      yes       source of input (see 'info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

[recon-ng][nk0741][hackertarget] > input

  +---------------+
  | Module Inputs |
  +---------------+
  | tesla.com     |
  +---------------+
```

Seting option source as “tesla.com” and printing the info about it.

```
[recon-ng][nk0741][hackertarget] > run

--------
TESLA.COM
--------
[*] Country: None
[*] Host: tesla.com
[*] Ip_Address: 96.16.108.43
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------------
[*] Country: None
[*] Host: o7.ptr6980.tesla.com
[*] Ip_Address: 149.72.144.42
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------------
[*] Country: None
[*] Host: email1.tesla.com
[*] Ip_Address: 192.28.144.15
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------------
[*] Country: None
[*] Host: vpn1.tesla.com
[*] Ip_Address: 8.45.124.215
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------------
[*] Country: None
[*] Host: apacvpn1.tesla.com
[*] Ip_Address: 8.244.131.215
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------------
[*] Country: None
```

Running the module.

```
SUMMARY
-------
[*] 59 total (59 new) hosts found.
[recon-ng][nk0741][hackertarget] > show hosts

  +-------------------------------------------------------------------------------------------------------------------------------+
  | rowid |             host             |    ip_address    | region | country | latitude | longitude | notes | module    |
  +-------------------------------------------------------------------------------------------------------------------------------+
  | 1     | tesla.com                    | 96.16.108.43     |        |         |          |           |       | hackertarget |
  | 2     | o7.ptr6980.tesla.com         | 149.72.144.42    |        |         |          |           |       | hackertarget |
  | 3     | email1.tesla.com             | 192.28.144.15    |        |         |          |           |       | hackertarget |
  | 4     | vpn1.tesla.com               | 8.45.124.215     |        |         |          |           |       | hackertarget |
  | 5     | apacvpn1.tesla.com           | 8.244.131.215    |        |         |          |           |       | hackertarget |
  | 6     | cnvpn1.tesla.com             | 114.141.176.215  |        |         |          |           |       | hackertarget |
  | 7     | vpn2.tesla.com               | 8.47.24.215      |        |         |          |           |       | hackertarget |
  | 8     | apacvpn2.tesla.com           | 124.158.21.195   |        |         |          |           |       | hackertarget |
  | 9     | model3.tesla.com             | 205.234.27.221   |        |         |          |           |       | hackertarget |
  | 10    | o3.ptr1444.tesla.com         | 149.72.152.236   |        |         |          |           |       | hackertarget |
  | 11    | mrsproxy06.tesla.com         | 209.11.133.58    |        |         |          |           |       | hackertarget |
  | 12    | o2.ptr556.tesla.com          | 149.72.134.64    |        |         |          |           |       | hackertarget |
```

Listing all the hosts of tesla.com. As we can see we have 59 hosts in total for tesla.com

Analysis:
After starting the recon-ng and installing the required modules we have set “tesla.com” as the source and ran the modules. The above screenshot shows the results.

Nikto:

Analysis:
The result of running the Nikto web server scanner against a target IP address (40.89.244.232) that corresponds to the domain "duckduckgo.com" on port 80 (HTTP).
Breaking down the key elements of the Nikto output:

0. Start Time:
The scan started at 2023-09-20 08:07:45 (GMT-4)
1. Information on Duckduckgo.com:
   Target IP: 40.89.244.232
   Target Hostname: duckduckgo.com
   Target Port: 80
2. Server Information:
   Server: nginx
   Root page / redirects to: https://duckduckgo.com/
   The target server is running the nginx web server software.
3. Headers:
   Several HTTP headers with uncommon names or contents were found. This can be an indicator of unusual or non-standard server configurations.
4. CGI Directories:
   No CGI directories were found on the server.
5. Robots.txt:
   The server's robots.txt file contains 10 entries. Robots.txt is used to specify which parts of a website should not be crawled or indexed by search engines. The entries should be manually reviewed to understand what's being restricted.

6. Multiple Index Files:
The server has multiple index files that can be used as the default page for directories. This includes common filenames like index.php, index.html, etc.

7. **Vulnerabilities and Security Issues:**

- Nikto has identified several potential vulnerabilities and security issues on the target server. These issues include:
    - Detection of an admin interface for the Cobalt Qube 3.
    - PHP-Survey's include file exposed via the web.
    - Detection of BigIP Configuration CGI.
    - Vulnerabilities in Macromedia JRun 4 build 61650 remote administration interface.
    - XSS (Cross-Site Scripting) vulnerability in IlohaMail 0.8.10.
    - Possible backdoor in Dansie Shopping Cart.
    - Detection of the Nimda virus in a readme.eml file.
    - Directory traversal vulnerability in Resin 2.1.2 view_source.jsp.
    - Potential issues with MySimpleNews and ASP file upload pages.
    - Exposure of .mdb database files in VP-ASP shopping cart applications.
    - Information disclosure in VP-ASP shopping cart test application.
    - Possible exposure of credit card data in webcart and webcart-lite configurations.
    - Detection of files like ws_ftp.ini, WS_FTP.ini, and whatever.htr that may reveal sensitive information.
    - More potential issues and vulnerabilities in various web applications and configurations.

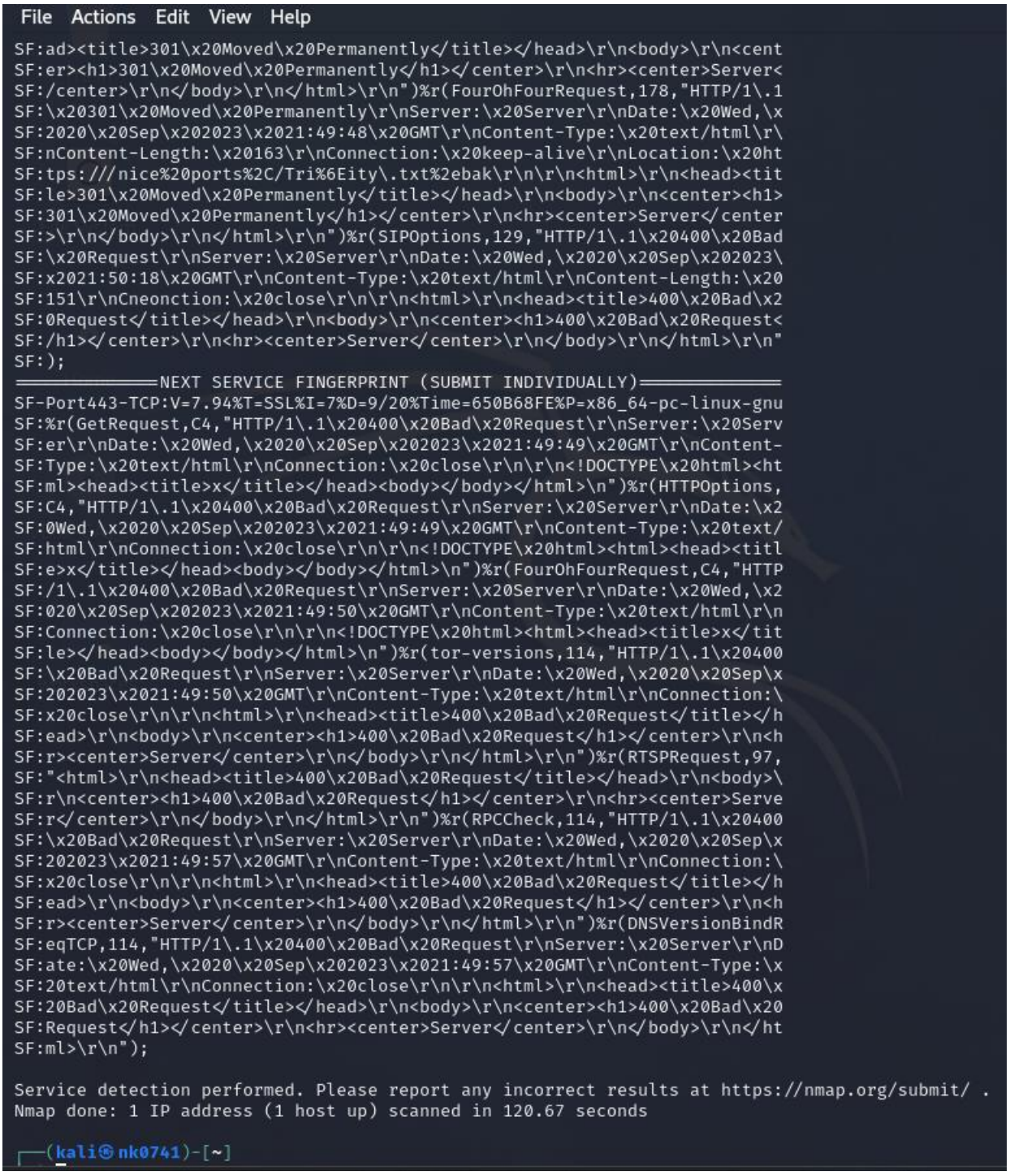
8. Scan Termination:
The scan terminated due to reaching an error limit of 20. The last error encountered was a timeout while trying to connect to the server.
9. End Time:
The scan ended at 2023-09-20 08:15:21 (GMT-4) after running for 456 seconds.

In summary, Nikto has identified a different potential security issues and vulnerabilities on the “duckduckgo.com” server, ranging from unusual headers and server configurations to specific vulnerabilities in various web applications and configurations. It's important to note that the presence of these issues does not necessarily mean the server is compromised, but it does highlight areas that may require further investigation and security hardening to reduce potential risks. The server administrators should review and address these findings to enhance the server's security posture.


nikto -h duckduckgo.com
- Nikto v2.5.0
+ Target IP: 40.89.244.232
+ Target Hostname: duckduckgo.com
+ Target Port: 80
+ Start Time: 2023-09-20 08:07:45 (GMT-4)
+ Server: nginx
+ Root page / redirects to: https://duckduckgo.com/
+ /45fAgFqZ.en: Uncommon header 'x-duckduckgo-result und, with contents: 1.
+ /45fAgFqZ.en: Uncommon header 'server-timing' found, with contents: total;dur=34;desc="Backend Total".
+ /45fAgFqZ.en: Uncommon header 'x-duckduckgo-locale nd, with contents: en_US.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: contains 10 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Gl
ossary/Robots.txt
+ Multiple index f ound: /index.php, /index.php7, /default.htm, /index.asp, /index.jhtml, /index.php4, /index.p
hp5, /index.jsp, /index.php3, /index.cfm, /default.asp, /index.xml, /index.aspx, /index.shtml, /index.cgi, /index.ht
m, /default.aspx, ex.html, /index.do.
+ /splashAdmin.php: Cobalt Qube 3 admin is running. This may have multiple security problems which could not be test
ed remotely. See: https://seclists.org/bugtraq/2002/Jul/262
+ /global.inc: PHP-Survey's include file should not be avail eb. Configure the web server to ignore .in
c files or change this to global.inc.php. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0614
+ /bigconf.cgi: BigIP Configuration CGI.
+ /clusterframe.jsp: Macromedia JRun 4 build 61650 remote administration interface is vulnerable to several XSS atta
cks.
+ /IlohaMail/blank.html: IlohaMail 0.8.10 contains a XSS vulnerability. Previous versions contain other non-descript
vulnerabilities.
+ /cartcart.cgi: If this is Dansie Shopping Cart 3.0.8 or earlier, it contains a backdoor to allow attackers to exec
ute arbitrary commands.
+ /readme.eml: Remote server may be infected with the Nimda virus.
+ /view_source.jsp: Resin 2.1.2 view_source.jsp allows any file on the system to be viewed by using \..\ directory t
raversal. This script may be vulnerable.
oaded via the web. These should not be available. See: https://securitytracker.com/id/1004382
+ /contents.php?new_language=elvish&mode=select: Requesting a file with an invalid language m DC Portal
may reveal the system path.
+ /shopa_sessionlist.asp: VP-ASP shopping cart test application is available from the web. the lo
cation of .mdb files which may also be available.
+ /vchat/msg.txt: VChat allows user information to be retrieved. See: https://www.securityfocus.com/bid/7186/info
+ /webcart-lite/config/import.txt: This may allow attackers to read credit card data. Recon ile
not accessible via the web. See: https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /webcart-lite/orders/import.txt: This may allow attackers to read credit card data. Recon file
not accessible via the web. See: https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /webcart/config/clients.txt: This may allow attackers to read credit card data. Recon file not
accessible via the web. See: https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /webcart/orders/import.txt: This may allow attackers to read credit card data. Recon s file not a
ccessible via the web. See: https://packetstormsecurity.com/files/32406/xmas.txt.html
+ /ws_ftp.ini: Can contain saved passwords for FTP sites.
+ /WS_FTP.ini: Can contain saved passwords for FTP sites.
+ /whatever.htr: May reveal physical path. htr files may also be vulnerable to an off-by-one overflow that allo
mote command execution. See: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2002/MS02-018
+ /webmail/blank.html: IlohaMail 0.8.10 contains an XSS vulnerabil versions contain other non-descript
vulnerabilities.
+ /quikstore.cfg: Shopping cart config file, http://www.quikstore.com/, nindsec.com/advisories/post2.txt.
See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0607
+ /quikstore.cgi: A shopping cart.
+ /smg_Smxcfg30.exe?vcc=3560121183d3: This may b rend Micro Officescan 'backdoor'.
+ /LOGIN.PWD: MIPCD password file with unencrypted passwords. MIPDCD should not have the web interface enabled.
+ /WebAdmin.dll?View=Logon: Some versions of Web nin are vulnerable to a remote DoS (not tested). See: http://cve.m
itre.org/cgi-bin/cvename.cgi?name=CVE-2005-1247
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect (timeout): Operatio
n now in progress
+ Scan terminated: 20 error(s) and 37 item(s) reported on remote host
+ End Time: 2023-09-20 08:15:21 (GMT-4) (456 seconds)
+ 1 host(s) tested

Nmap:

```
Compiled without:
Available nsock engines: epoll poll select

┌──(kali㉿nk0741)-[~]
└─$ nmap kmit.in
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-20 17:35 EDT
Failed to resolve "kmit.in".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 14.26 seconds

┌──(kali㉿nk0741)-[~]
└─$ nmap amazon.com
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-20 17:36 EDT
Nmap scan report for amazon.com (52.94.236.248)
Host is up (0.040s latency).
Other addresses for amazon.com (not scanned): 54.239.28.85 205.251.242.103
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 4.69 seconds

┌──(kali㉿nk0741)-[~]
└─$ nmap -T4 -A amazon.in
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-20 17:49 EDT
Nmap scan report for amazon.in (52.95.116.115)
Host is up (0.13s latency).
Other addresses for amazon.in (not scanned): 52.95.120.67 54.239.33.92
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE   VERSION
80/tcp  open  http      Server
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 301 Moved Permanently
|     Server: Server
|     Date: Wed, 20 Sep 2023 21:49:48 GMT
|     Content-Type: text/html
|     Content-Length: 163
|     Connection: keep-alive
|     Location: https:///nice%20ports%2C/Tri%6Eity.txt%2ebak
|     <html>
|     <head><title>301 Moved Permanently</title></head>
|     <body>
|     <center><h1>301 Moved Permanently</h1></center>
|     <hr><center>Server</center>
|     </body>
|     </html>
|   GetRequest:
```



In first instance, Nmap attempted to scan the domain "kmit.in". However, it was unable to resolve the domain to an IP address. This can happen if the domain name is not valid, doesn't exist, or if there are DNS resolution issues.

In second instance, Nmap successfully resolved the domain "amazon.com" to its corresponding IP address (52.94.236.248) using DNS. It then performed a basic Nmap scan on the specified IP address.The scan revealed that the host is up with a latency of 0.040 seconds.
It identified open ports:
Port 80: Open, likely for HTTP services.
Port 443: Open, likely for HTTPS services.
Additionally, it reported that there were 998 filtered TCP ports (no-response), meaning Nmap received no response for those ports.

SQLMap:

In one of instance, the target URL https://www.msgsafe.io/login

Breakdown of the output:

Warning and Disclaimer:

The output starts with a warning and legal disclaimer, highlighting the responsibility of the user to obey all applicable laws and the potential misuse or damage that could occur from using SQLMap without proper authorization.

Target URL without Parameters:
SQLMap warns that the provided target URL does not have any GET parameters. It asks if you want to try URI injections in the target URL itself.

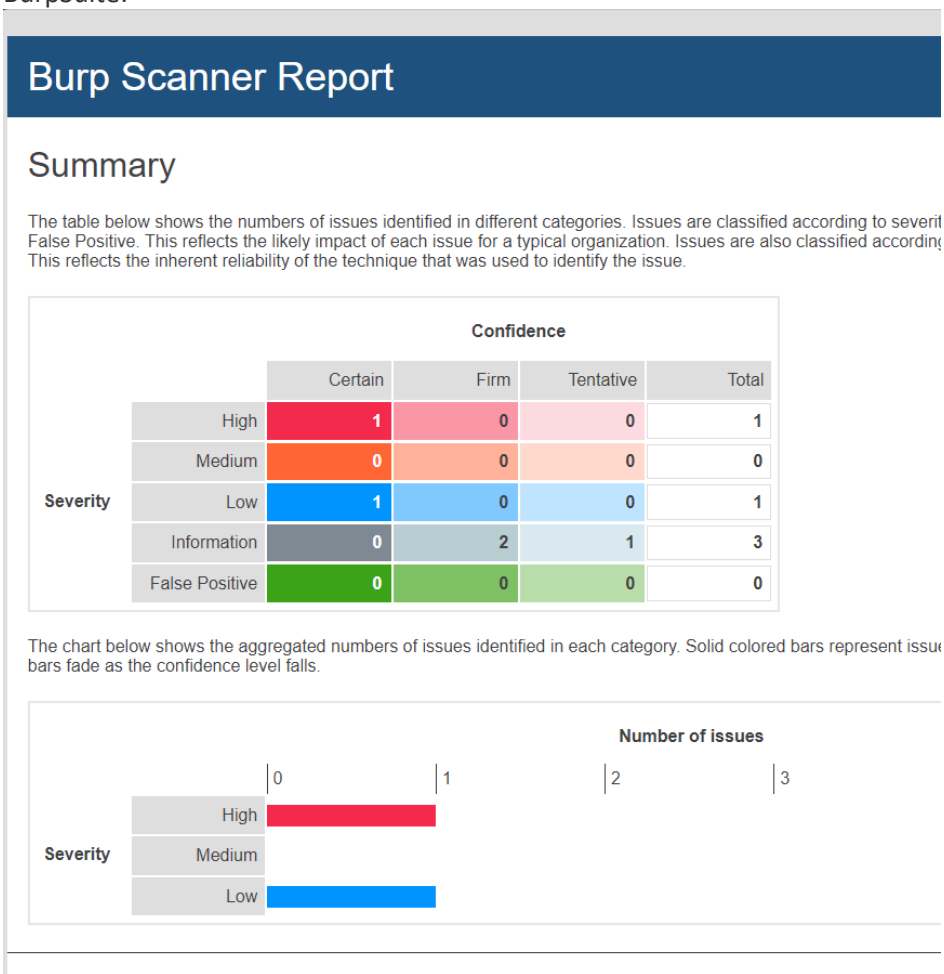
Connection and Stability Checks:
SQLMap tests the connection to the target URL, checks for Web Application Firewall (WAF) or Intrusion Prevention System (IPS) protection, and verifies the stability of the target URL's content.

Dynamic Parameter Detection:
SQLMap detects a potentially dynamic URI parameter ('#1*') and proceeds to test if it's injectable for SQL injection.

SQL Injection Testing:
SQLMap tests various SQL injection techniques such as boolean-based blind, error-based, time-based blind, and UNION-based queries to determine if the detected URI parameter is vulnerable to SQL injection.

Result and Recommendation:
SQLMap concludes that the tested parameters do not appear to be injectable. It suggests increasing values for '--level'/'--risk' options if you wish to perform more tests and advises trying different tamper options or switching '--random-agent'.

BurpSuite:



Burp Scanner Report

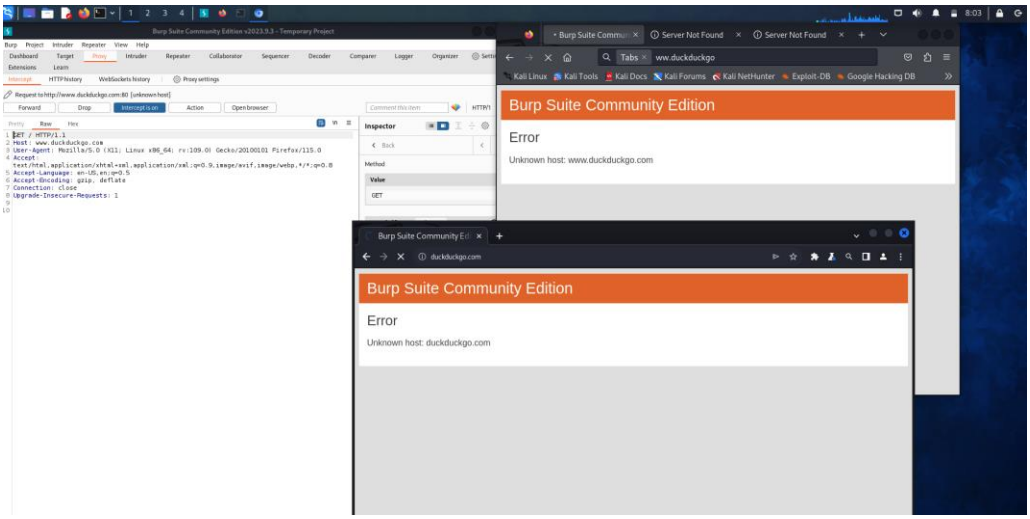
Summary

The table below shows the numbers of issues identified in different categories. Issues are classified according to severit
False Positive. This reflects the likely impact of each issue for a typical organization. Issues are also classified according
This reflects the inherent reliability of the technique that was used to identify the issue.

		Confidence			
		Certain	Firm	Tentative	Total
Severity	High	1	0	0	1
	Medium	0	0	0	0
	Low	1	0	0	1
	Information	0	2	1	3
	False Positive	0	0	0	0

The chart below shows the aggregated numbers of issues identified in each category. Solid colored bars represent issue
bars fade as the confidence level falls.

This is the Burpsuite report we generated using the professional version for learning the usage of burpsuite.



In the above screenshot, I used burpsuite community edition to intercept the browser when trying to open duckduckgo.com and able to intercept the request using burpsuite. I configured the firefox proxy for it and we can do the same using the inbuild chromium browser for this as well. The two windows on the right are firefox and chromium browsers.

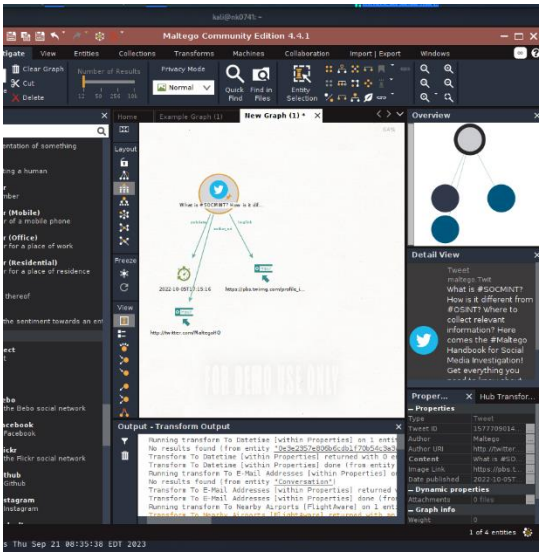
Part B: Passive Reconnaissance with Reconnaissance Tools

The Harvester

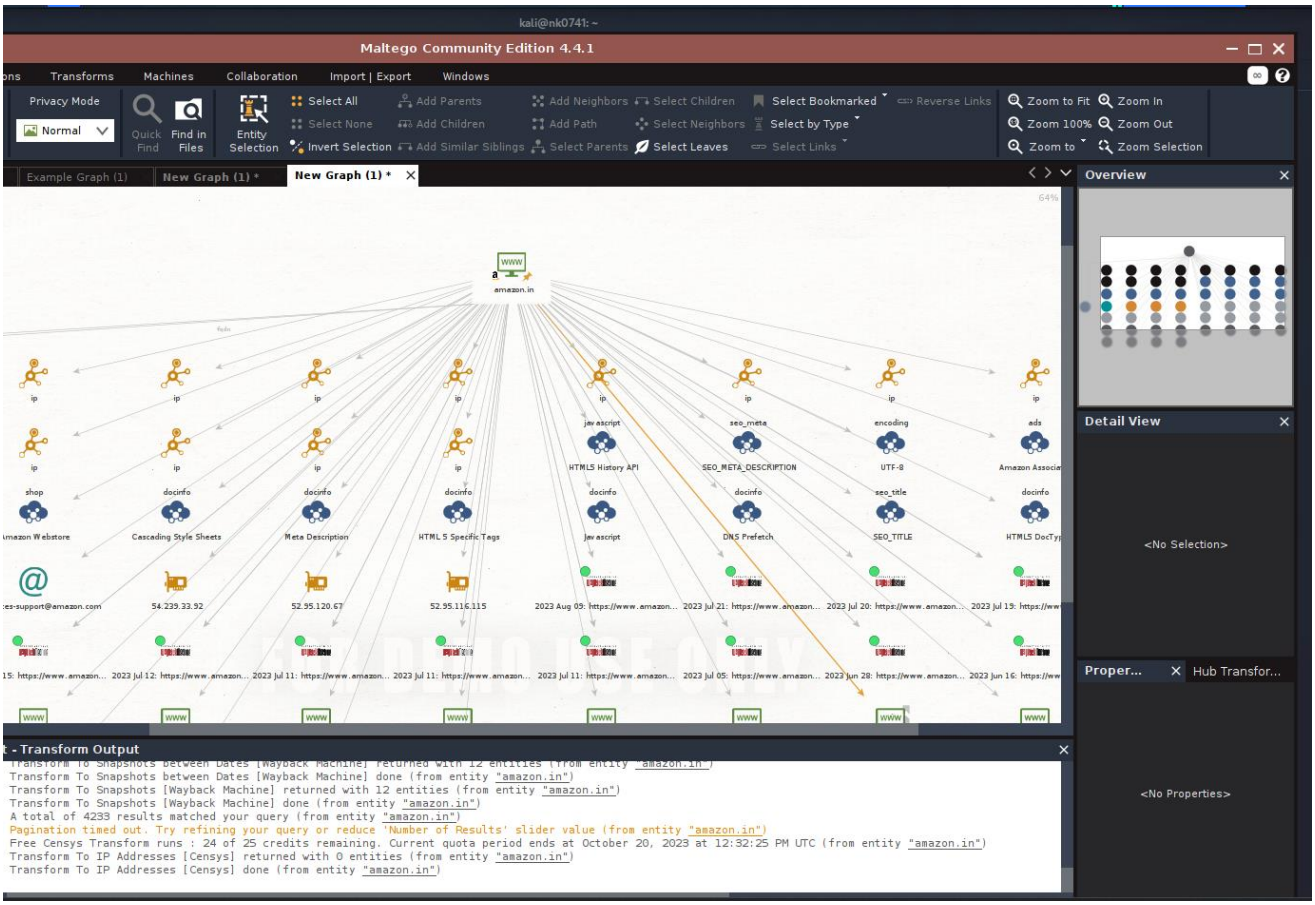
```
[*] ASNS found: 2
--------------------
AS13335
AS40824

[*] Interesting Urls found: 1
-----------------------------
https://kmit.in/

[*] LinkedIn Links found: 0
---------------------------

[*] IPs found: 7
----------------
104.155.227.88
206.54.190.30
208.88.226.229
2606:4700:30::6818:76ca
52.177.185.15

[*] Emails found: 4
-------------------
'@kmit.in
info@kmit.in
learner@kmit.in
resumes@kmit.in

[*] Hosts found: 13
-------------------
alumni.kmit.in
alumni.kmit.in:kmit.almabaseapp.com
alumni.kmit.in:kmit.almabaseapp.com.
alumni.kmit.in:mx.sendgrid.net
elms.kmit.in:206.54.190.30
kmit.in:mail.kmit.in
kmit.in:mail.kmit.in.
kmitra.kmit.in:206.54.190.30
mail.kmit.in
mail.kmit.in:3.231.172.249
mail.kmit.in:mail.kmit.in
student.kmit.in
student.kmit.in:206.54.190.30

┌──(kali㉿nk0741)-[~]
```

Analysis:
Here TheHarvester attempted to gather information such as emails, subdomains, hosts, ASNs (Autonomous System Numbers), interesting URLs, and LinkedIn links related to the domain "kmit.in". 7 IP addresses and 4 email addresses were identified as associated with the domain "kmit.in". The last list in the screenshot is the list of sub domains along with their IP addressess.

Maltego : Below is the screenshot of using transform to find details on a tweet using maltego.



In this we used maltego to get all the ip addresses, metadata descriptors, server address that are linked to amazon.in using Censys and ip transforms.



Spider Foot

We used spriderfoot to make it go through the meesho.com website.

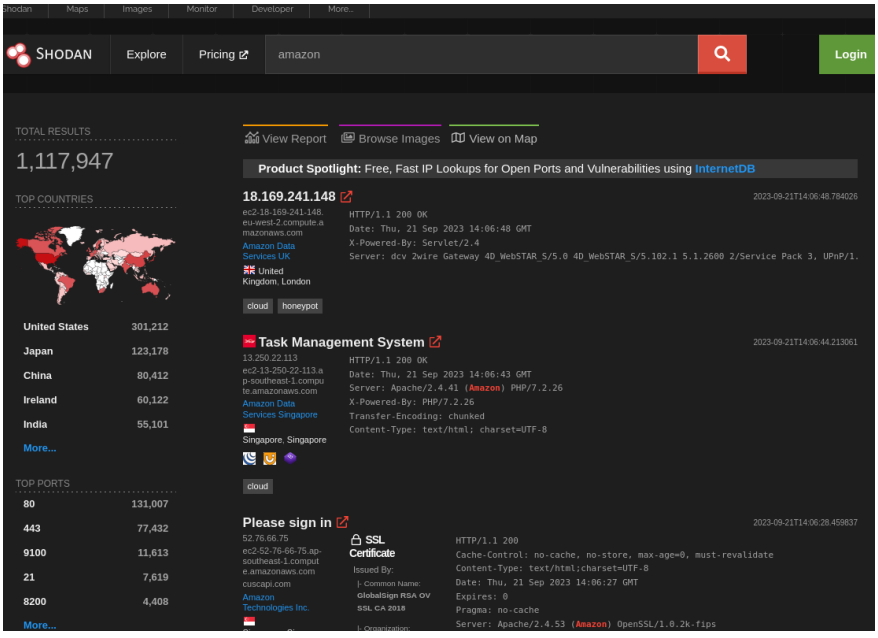
```
┌──(kali㉿nk0741)-[~]
└─$ spiderfoot -s meesho.com
2023-09-21 09:55:30,934 [WARNING] sf : You didn't specify any modules, types or use case, so all modules will be enabled.
Source                          Type                                    Data
2023-09-21 09:55:30,936 [INFO] sf : Modules enabled (235): sfp_sociallinks,sfp_archiveorg,sfp_whoxy,sfp_dnsneighbor,sfp_instagram,sfp_searchcode,sfp_abuseipdb,sfp_badpackets,sfp_callername,sfp_tool_snallygaster,sfp_torch,sfp_adguard_dns,sfp_errors,sfp_zoneh,sfp_dnsresolve,sfp_citadel,sfp_certspotter,sfp_phishstats,sfp_tool_nbtscan,sfp_hybrid_analysis,sfp_botscout,sfp_social,sfp_whoisology,sfp_dns_for_family,sfp_scylla,sfp_multiproxy,sfp_maltiverse,sfp_twitter,sfp_twilio,sfp_ipstack,sfp_riskiq,sfp_tool_whatweb,sfp_torexits,sfp_xforce,sfp_gravatar,sfp_blocklistde,sfp_nameapi,sfp_onioncity,sfp_censys,sfp_snov,sfp_reversewhois,sfp_tool_nmap,sfp_googleobjectstorage,sfp_isc,sfp_arin,sfp_haveibeenpwned,sfp_spider,sfp_hashes,sfp_spamcop,sfp_webanalytics,sfp_skymem,sfp_fsecure_riddler,sfp_spur,sfp_company,sfp_textmagic,sfp_crobat_api,sfp_dehashed,sfp_bitcoinabuse,sfp_openbugbounty,sfp_hosting,sfp_grayhatwarfare,sfp_trumail,sfp_cloudfraredns,sfp_circllu,sfp_greynoise,sfp_ipqualityscore,sfp_flickr,sfp_hunter,sfp_spamhaus,sfp_ipapico,sfp_talosintel,sfp_crossref,sfp_debounce,sfp_ahmia,sfp_googlemaps,sfp_yandexdns,sfp_names,sfp_cybercrimetracker,sfp_opencorporates,sfp_duckduckgo,sfp_socialprofiles,sfp_ripe,sfp_bingsearch,sfp_numverify,sfp_ipregistry,sfp_base64,sfp_alienvault,sfp_digitaloceanspace,sfp_threatcrowd,sfp_openphish,sfp_iban,sfp_jsonwhoiscom,sfp_accounts,sfp_apple_itunes,sfp_sublist3r,sfp_onionsearchengine,sfp_botvrij,sfp_dnsbrute,sfp_tool_retirejs,sfp_ipapicom,sfp_binaryedge,sfp_virustotal,sfp_s3bucket,sfp_uceprotect,sfp_seon,sfp_commoncrawl,sfp_comodo,sfp_punkspider,sfp_robtex,sfp_tool_testsslsh,sfp_countryname,sfp_similar,sfp_onyphe,sfp_cleantalk,sfp_tool_trufflehog,sfp_shodan,sfp_vxvault,sfp_portscan_tcp,sfp_darksearch,sfp_filemeta,sfp_dnsdb,sfp_phishtank,sfp_grep_app,sfp_cleanbrowsing,sfp_surbl,sfp_adblock,sfp_dnsgrep,sfp_zetalytics,sfp_viewdns,sfp_recondev,sfp_intfiles,sfp_gleif,sfp_ipinfo,sfp_open_passive_dns_database,sfp_alienvaultiprep,sfp_pgp,sfp_koodous,sfp_neutrinoapi,sfp_wigle,sfp_focsec,sfp_hostio,sfp_emailformat,sfp_emailrep,sfp_strangeheaders,sfp_tldsearch,sfp_hackertarget,sfp_leakix,sfp_networksdb,sfp_dnscommonsrv,sfp_bitcoinwhoswho,sfp_slideshare,sfp_keybase,sfp_webserver,sfp_mnemonic,sfp_dronebl,sfp_fraudguard,sfp_pastebin,sfp_venmo,sfp_azureblobstorage,sfp_binstring,sfp_bgpview,sfp_phone,sfp_email,sfp_tool_cmseek,sfp_opens treetmap,sfp_spyonweb,sfp_bitcoin,sfp_pageinfo,sfp_abusix,sfp_etherscan,sfp_cookie,sfp_fullhunt,sfp_dnszonexfer,sfp_honeypot,sfp_abusech,sfp_voipbl,sfp_tool_dnstwist,sfp_dnsdumpster,sfp_bingsharedip,sfp_coinblocker,sfp_urlscan,sfp_stackoverflow,sfp_sorbs,sfp_c99,sfp_spyse,sfp_ethereum,sfp_fullcontact,sfp_wikileaks,sfp_whatcms,sfp_junkfiles,sfp_abstractapi,sfp_subdomain_takeover,sfp_myspace,sfp_malwarepatrol,sfp_openonic,sfp_creditcard,sfp_emailcrawlr,sfp_fortinet,sfp_tool_nuclei,sfp_crxcavator,sfp_opendns,sfp_blockchain,sfp_quad9,sfp_emergingthreats,sfp_threatminer,sfp_googlesearch,sfp_greensnow,sfp_pulsedive,sfp_iknowwhatyoudownload,sfp_cinsscore,sfp_metadefender,sfp_clearbit,sfp_securitytrails,sfp_h1nobbdde,sfp_customfeed,sfp_dnsraw,sfp_threatfox,sfp_stevenblack_hosts,sfp_tool_onesixtyone,sfp_projectdiscovery,sfp_googlesafebrowsing,sfp_wikipediaedits,sfp_psbdmp,sfp_tool_wappalyzer,sfp_github,sfp_whois,sfp_crt,sfp_tool_wafw00f,sfp_sslcert,sfp_webframework,sfp_intelx,sfp_trashpanda,sfp_builtwith,sfp__stor_db,sfp__stor_stdout
2023-09-21 09:55:31,745 [INFO] sflib : Downloading configuration data from: https://publicsuffix.org/list/effective_tld_names.dat
2023-09-21 09:55:31,918 [INFO] sflib : Scan [A6270728] for 'meesho.com' initiated.
2023-09-21 09:55:31,925 [INFO] sflib : sfp_sociallinks module loaded.
2023-09-21 09:55:31,931 [INFO] sflib : sfp_archiveorg module loaded.
2023-09-21 09:55:31,938 [INFO] sflib : sfp_whoxy module loaded.
2023-09-21 09:55:31,944 [INFO] sflib : sfp_dnsneighbor module loaded.
2023-09-21 09:55:31,949 [INFO] sflib : sfp_instagram module loaded.
2023-09-21 09:55:31,954 [INFO] sflib : sfp_searchcode module loaded.
2023-09-21 09:55:31,960 [INFO] sflib : sfp_abuseipdb module loaded.
2023-09-21 09:55:31,965 [INFO] sflib : sfp_badpackets module loaded.
2023-09-21 09:55:31,970 [INFO] sflib : sfp_callername module loaded.
2023-09-21 09:55:31,975 [INFO] sflib : sfp_tool_snallygaster module loaded.
2023-09-21 09:55:31,980 [INFO] sflib : sfp_torch module loaded.
```

From below screenshot we get the information all the product listed in it and dns list. In the next screenshot containing the details of the digital certs used by meesho and there public details.

```
areDeveloper&limit=100&term=com.meesho (proxy=None, user-agent=Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.
0, timeout=5, cookies=None)
2023-09-21 09:55:36,943 [INFO] sflib : Fetched https://www.zone-h.org/rss/specialdefacements (8156 bytes in 0.19774103164672852s)
2023-09-21 09:55:36,944 [INFO] sflib : Fetching (GET): https://www.threatcrowd.org/searchApi/v2/domain/report/?domain=meesho.com (proxy=None
, user-agent=SpiderFoot, timeout=5, cookies=None)
sfp_dnsresolve                  IP Address                                      18.140.90.80
sfp_dnsresolve                  Domain Name                                     meesho.com
sfp_dnsresolve                  IP Address                                      54.251.215.6
sfp_dnsresolve                  IP Address                                      18.140.23.75
2023-09-21 09:55:37,177 [INFO] sflib : Fetched https://searchcode.com/api/codesearch_I/?q=meesho.com&p=0&per_page=100 (59 bytes in 0.5027310
848236084s)
2023-09-21 09:55:37,249 [ERROR] sflib : Failed to connect to https://www.threatcrowd.org/searchApi/v2/domain/report/?domain=meesho.com
2023-09-21 09:55:37,249 [INFO] sfp_threatcrowd : No ThreatCrowd info found for meesho.com
2023-09-21 09:55:37,409 [INFO] sflib : Fetching (GET): https://scylla.so/search?q=email%3A%40meesho.com&size=20&start=0 (proxy=None, user-ag
ent=Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0, timeout=15, cookies=None)
2023-09-21 09:55:37,859 [INFO] sflib : Fetched https://itunes.apple.com/search?media=software&entity=software%2CiPadSoftware%2CsoftwareDevel
oper&limit=100&term=com.meesho (351601 bytes in 0.9257142543792725s)
2023-09-21 09:55:37,958 [INFO] sflib : Fetched https://scylla.so/search?q=email%3A%40meesho.com&size=20&start=0 (3067 bytes in 0.54871511459
35059s)
2023-09-21 09:55:38,864 [INFO] sflib : Fetching (GET): https://www.threatcrowd.org/searchApi/v2/ip/report/?ip=18.140.90.80 (proxy=None, user
-agent=SpiderFoot, timeout=5, cookies=None)
sfp_apple_itunes                App Store Entry                                 Meesho:Online Shopping 2.48 (com.meesho.Meesho)
https://apps.apple.com/us/app/meesho-online-shopping/id1457958492?uo=4
sfp_apple_itunes                Linked URL - Internal                           https://meesho.com/
```

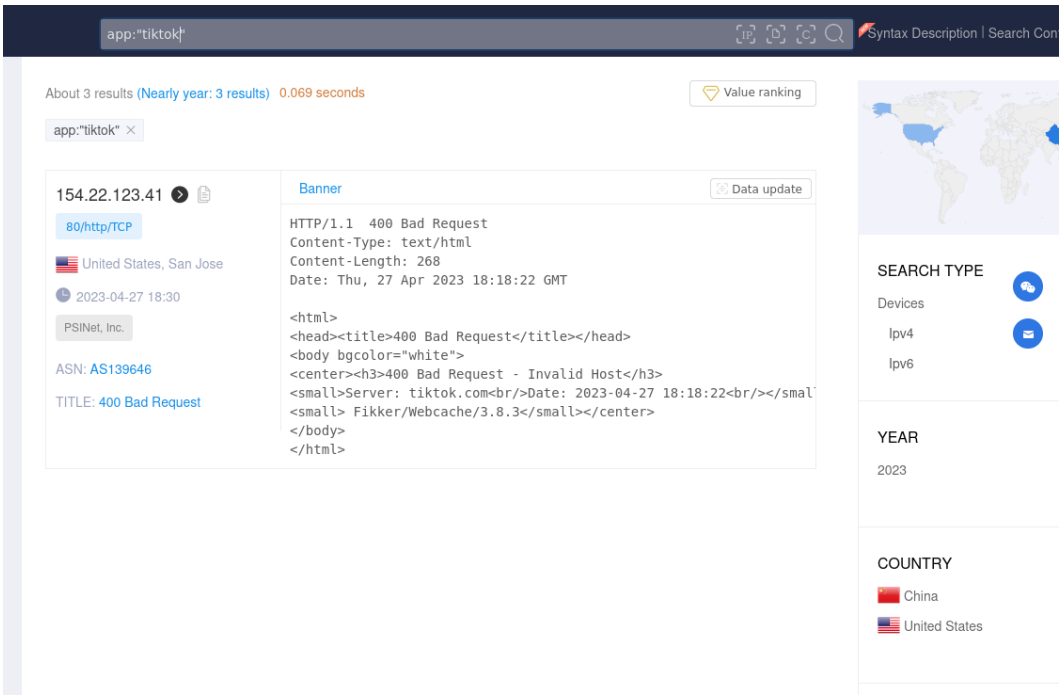
```
sfp_crt                         Internet Name                                   www.meesho.com
sfp_crt                         Co-Hosted Site                                  sni.cloudflaressl.com
2023-09-21 10:17:06,234 [INFO] sfp_tldsearch : Spawning threads to check TLDs: [['meesho.e', 'e'], ['meesho.d', 'd'], ['meesho.b', 'b'], ['m
eesho.y', 'y']]
2023-09-21 10:17:06,439 [INFO] sfp_tldsearch : Spawning threads to check TLDs: [['meesho.e', 'e'], ['meesho.g', 'g'], ['meesho.i', 'i'], ['m
eesho.s', 's']]
2023-09-21 10:17:06,620 [INFO] sflib : Fetched https://crt.sh/?d=7103235273 (1891 bytes in 0.5786290168762207s)
2023-09-21 10:17:06,649 [INFO] sfp_tldsearch : Spawning threads to check TLDs: [['meesho.r', 'r'], ['meesho.y', 'y'], ['meesho.<', '<'], ['m
eesho.j', 'j']]
sfp_crt                         SSL Certificate - Raw Data                      Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            04:60:69:73:a0:fc:41:f7:33:f0:f5:a9:25:fb:0c:76
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Cloudflare, Inc., CN=Cloudflare Inc RSA CA-2
        Validity
            Not Before: Jul 11 00:00:00 2022 GMT
            Not After : Jul 10 23:59:59 2023 GMT
        Subject: C=US, ST=California, L=San Francisco, O=Cloudflare, Inc., CN=sni.cloudflaressl.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:9f:68:0f:ca:ac:61:0d:e3:74:6e:b2:e1:01:01:
                    f7:47:3a:52:7a:bf:8b:32:ed:dc:05:0b:13:46:bb:
                    c4:bb:ae:d5:6c:1a:93:49:e3:5e:5e:7c:2b:f6:e8:
                    1b:41:4b:8b:4b:40:27:f3:68:01:75:17:b6:ca:5e:
                    54:65:fd:32:5e:2d:e9:67:f3:0c:73:2f:4f:cf:67:
                    ac:64:bc:05:25:df:a6:7f:c0:7c:58:da:c6:ad:85:
                    34:6a:6c:25:78:f1:ae:2b:3f:5c:90:af:63:9f:8e:
                    c3:2f:07:09:a3:18:0c:cf:b1:e1:b4:6e:1c:5e:2c:
                    17:f6:95:42:48:49:ee:24:94:fb:00:e5:c4:f1:ca:
                    80:8d:63:bc:c4:ac:12:c0:71:5c:00:8d:50:3e:ca:
                    68:0e:9e:b4:91:03:39:31:76:64:92:d1:b8:aa:96:
                    f3:f3:79:56:a8:3f:19:d8:80:c4:b4:8b:c2:67:bc:
                    1a:05:5a:d5:5d:34:96:b5:7f:fe:f8:ff:42:c0:3e:
                    96:71:a6:8b:8a:e4:cc:ad:03:e2:b1:64:a4:80:c0:
                    c6:34:f7:21:b3:44:03:af:f7:1b:b4:8e:00:2d:da:
                    73:1b:fb:28:e9:8d:63:b2:3b:55:e2:4a:10:c7:79:
                    48:00:dc:2d:cf:a7:72:8b:d9:35:63:2f:a4:73:e9:
                    9a:df
                Exponent: 65537 (0x10001)
        X509v3 extensions:
```

Shodan

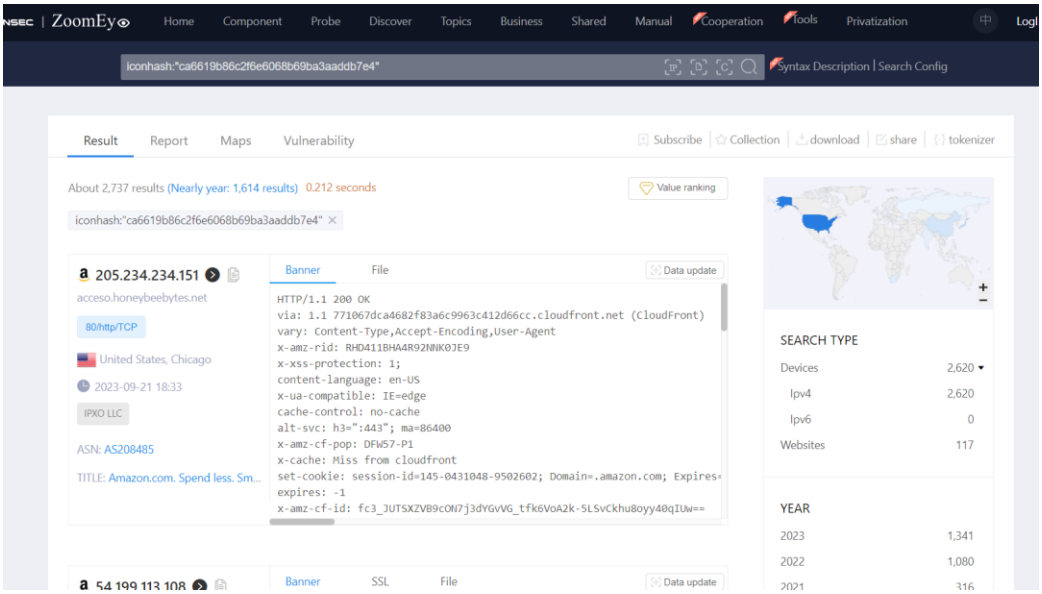


It gives info on list of servers and their IP addresses country they are present and ports which are used by it and many other details. We can even view IP cameras which are public.

ZoomEye.org: It is a search engine specifically designed for discovering and visualizing IoT (Internet of Things) devices, services, and vulnerabilities. It is primarily used for gathering open-source intelligence (OSINT) related to IoT devices and associated network services

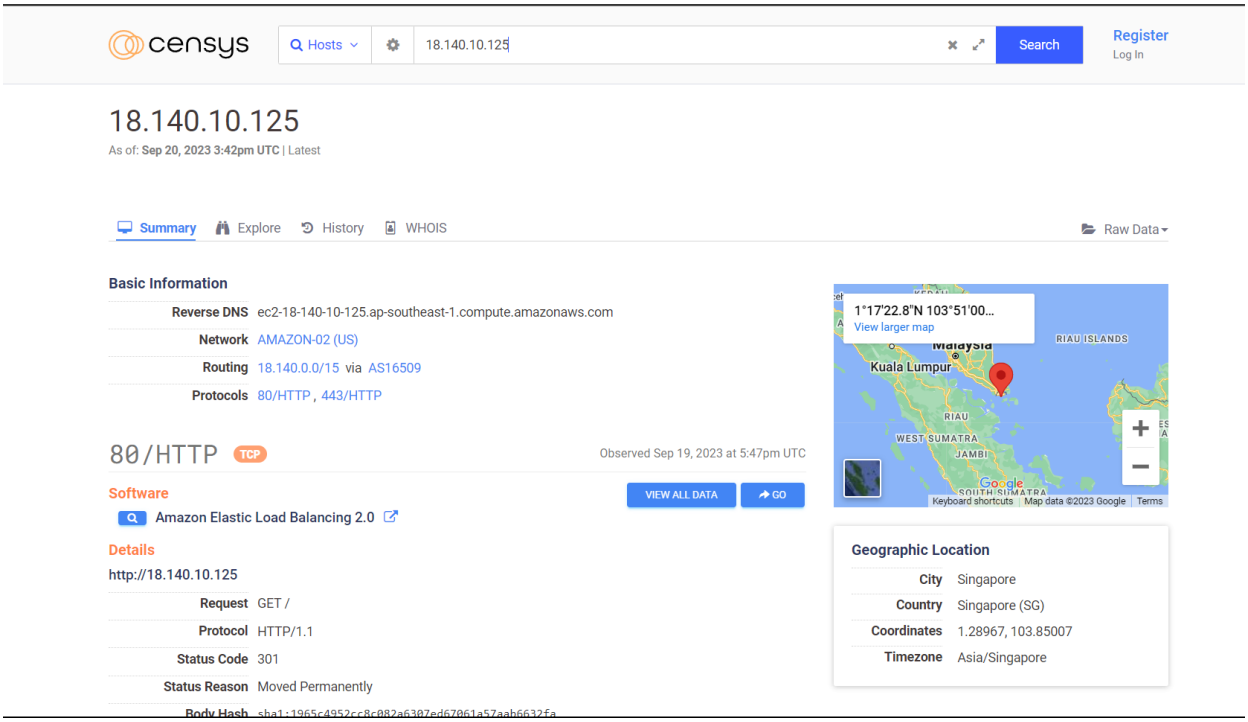


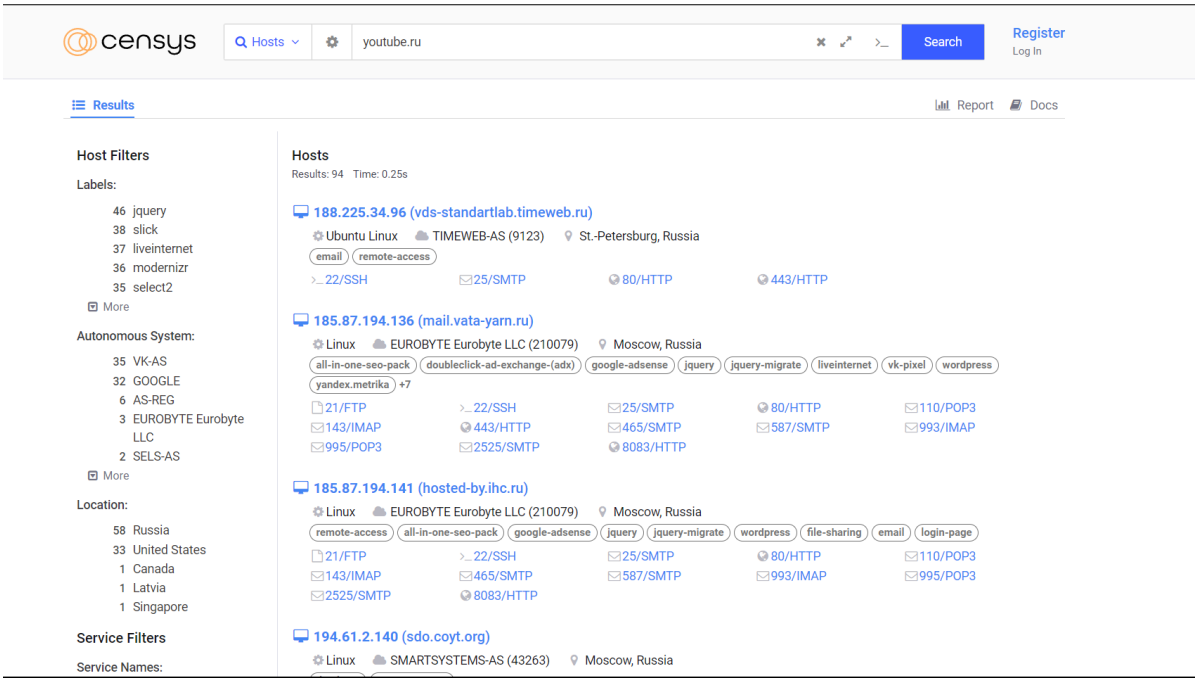
We can the iconhash for searching as well using zoomeye. Below is the screenshot where we amazon icon for doing the search.



Censys.io

It gives the details where ip address is orginated and reverse dns, who it belongs to. Incidently we give the url to get the details where it orginates and what all ip addresses and it has option to generate report depending on user need. I used to generate report for location where it servers are present in the last screenshot.


censys
Hosts
18.140.10.125
Search
Register
Log In
18.140.10.125
As of: Sep 20, 2023 3:42pm UTC | Latest
Summary
Explore
History
WHOIS
Raw Data
Basic Information
Reverse DNS ec2-18-140-10-125.ap-southeast-1.compute.amazonaws.com
Network AMAZON-02 (US)
Routing 18.140.0.0/15 via AS16509
Protocols 80/HTTP , 443/HTTP
80/HTTP TCP
Observed Sep 19, 2023 at 5:47pm UTC
Software
VIEW ALL DATA
GO
Amazon Elastic Load Balancing 2.0
Details
http://18.140.10.125
Request GET /
Protocol HTTP/1.1
Status Code 301
Status Reason Moved Permanently
Body Hash sha1:1965c4952cc8c082a6307ed67061a57aab6632fa
1°17'22.8"N 103°51'00...
View larger map
Kuala Lumpur
RIAU ISLANDS
RIAU
WEST SUMATRA
JAMBI
Google
Keyboard shortcuts
Map data ©2023 Google
Terms
Geographic Location
City Singapore
Country Singapore (SG)
Coordinates 1.28967, 103.85007
Timezone Asia/Singapore


censys
Hosts
youtube.ru
Search
Register
Log In
Results
Report
Docs
Host Filters
Labels:
46 jquery
38 slick
37 liveinternet
36 modernizr
35 select2
More
Autonomous System:
35 VK-AS
32 GOOGLE
6 AS-REG
3 EUROBYTE Eurobyte LLC
2 SELS-AS
More
Location:
58 Russia
33 United States
1 Canada
1 Latvia
1 Singapore
Service Filters
Service Names:
Hosts
Results: 94 Time: 0.25s
188.225.34.96 (vds-standartlab.timeweb.ru)
Ubuntu Linux TIMEWEB-AS (9123) St.-Petersburg, Russia
email remote-access
22/SSH 25/SMTP 80/HTTP 443/HTTP
185.87.194.136 (mail.vata-yarn.ru)
Linux EUROBYTE Eurobyte LLC (210079) Moscow, Russia
all-in-one-seo-pack doubleclick-ad-exchange-(adx) google-adsense jquery jquery-migrate liveinternet vk-pixel wordpress yandex.metrika +7
21/FTP 22/SSH 25/SMTP 80/HTTP 110/POP3
143/IMAP 443/HTTP 465/SMTP 587/SMTP 993/IMAP
995/POP3 2525/SMTP 8083/HTTP
185.87.194.141 (hosted-by.ihc.ru)
Linux EUROBYTE Eurobyte LLC (210079) Moscow, Russia
remote-access all-in-one-seo-pack google-adsense jquery jquery-migrate wordpress file-sharing email login-page
21/FTP 22/SSH 25/SMTP 80/HTTP 110/POP3
143/IMAP 465/SMTP 587/SMTP 993/IMAP 995/POP3
2525/SMTP 8083/HTTP
194.61.2.140 (sdo.coyt.org)
Linux SMARTSYSTEMS-AS (43263) Moscow, Russia

censys | Hosts | youtube.ru | Search | Register | Log In

Report on Hosts

This tool allows you to generate a report on the breakdown of a value present on the Hosts returned by your query. For example, to generate a report on ports seen on Hosts with HTTP services, you could query for `services.service_name: HTTP` and then generate a report on the breakdown of the field `services.port`

Breakdown Field: location.city

Number of Buckets: 50

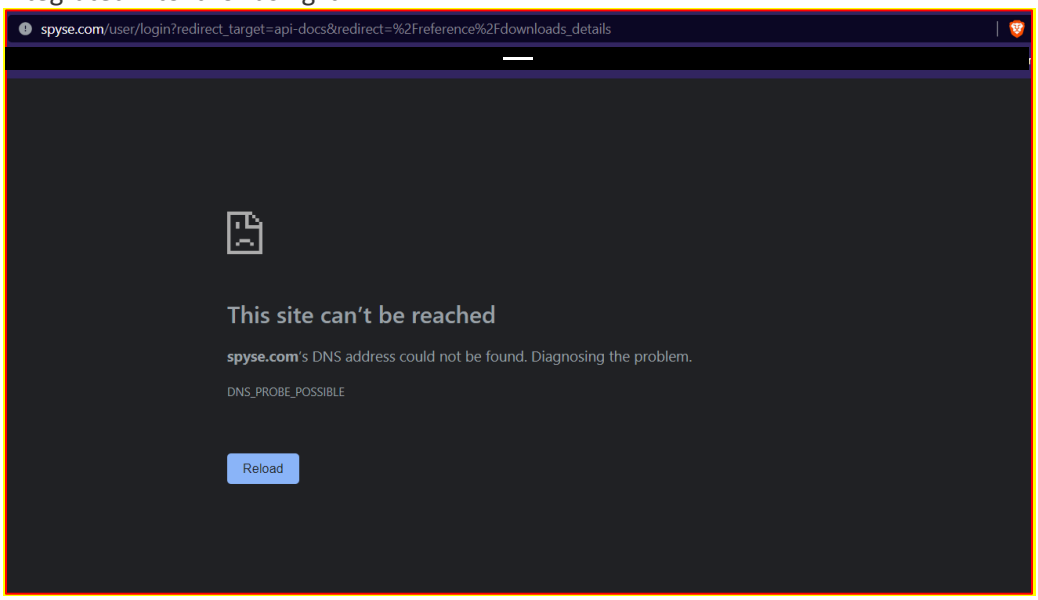
BUILD REPORT

Report for Hosts

location.city	hosts	
Moscow	50	53.19%
Atlanta	30	31.91%
Saint Petersburg	5	5.32%
Chicago	2	2.13%
Seversk	2	2.13%
Ashburn	1	1.06%
Beauharnois	1	1.06%
Kirov	1	1.06%
Riga	1	1.06%
Singapore	1	1.06%

Spyse.com

I think Spyse.com got shutdown and no longer available to use. Below u can sniper use various tools which are integrated into it for using it.



spyse-dev.readme.io/reference/quick-start

CTRL-/

SDKs & Integrations

CLI:

- Official CLI

SDK:

- Official SDK for Python
- Official SDK for Golang
- Community SDK for Ruby

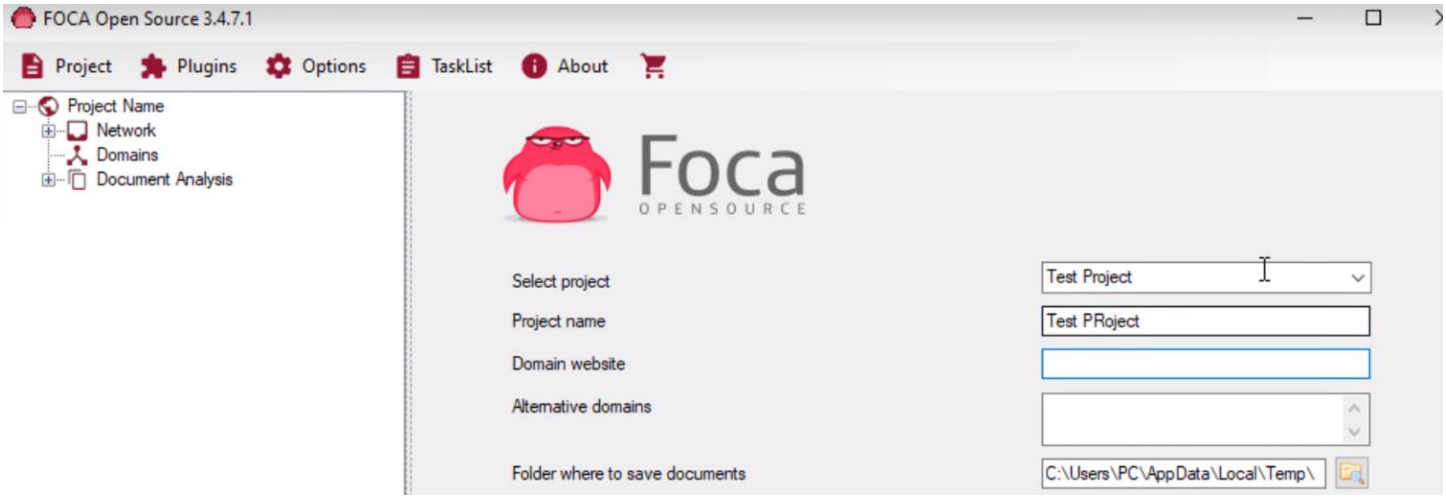
Integrations:

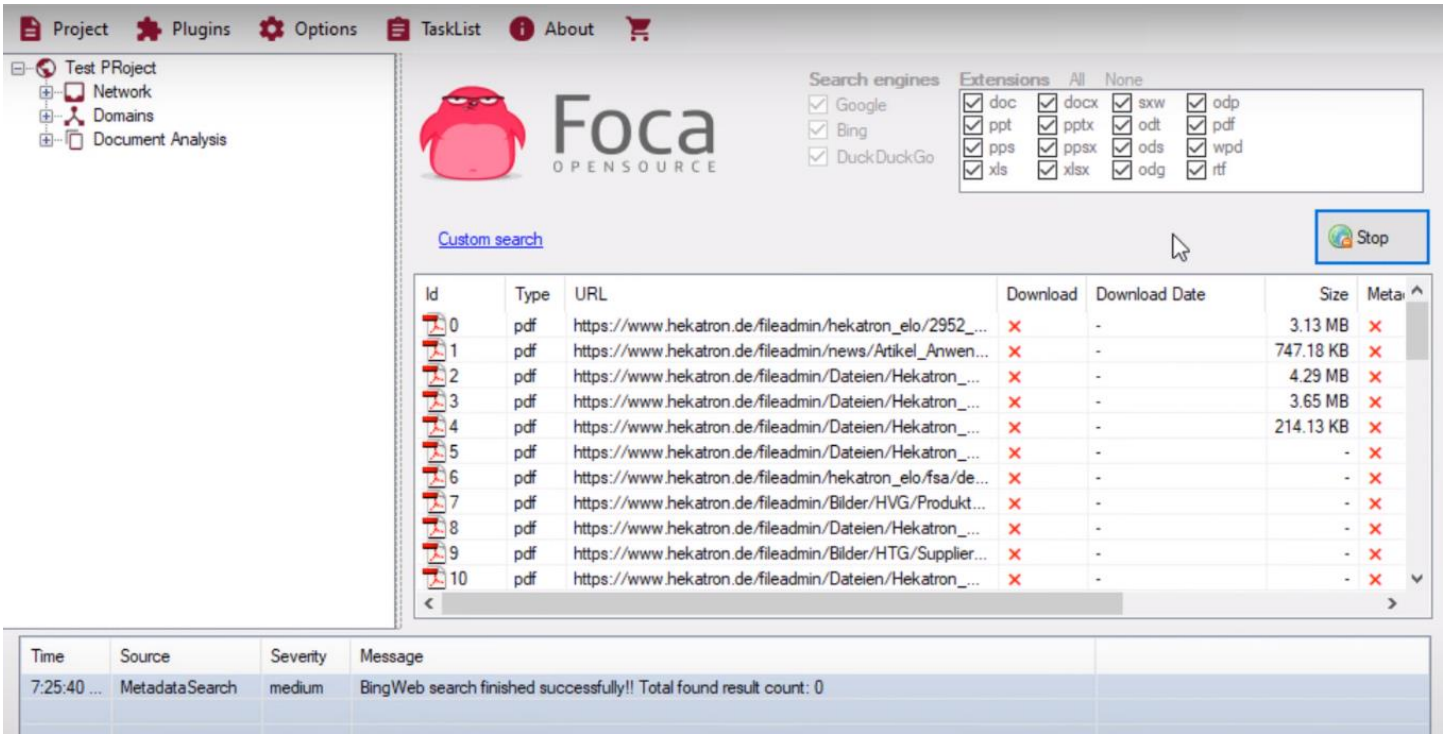
- Spiderfoot
- Amass
- theHarvester
- Subfinder
- IntelOwl
- Sudomy
- Mihari
- Sputnik
- Mitaka

Pricing

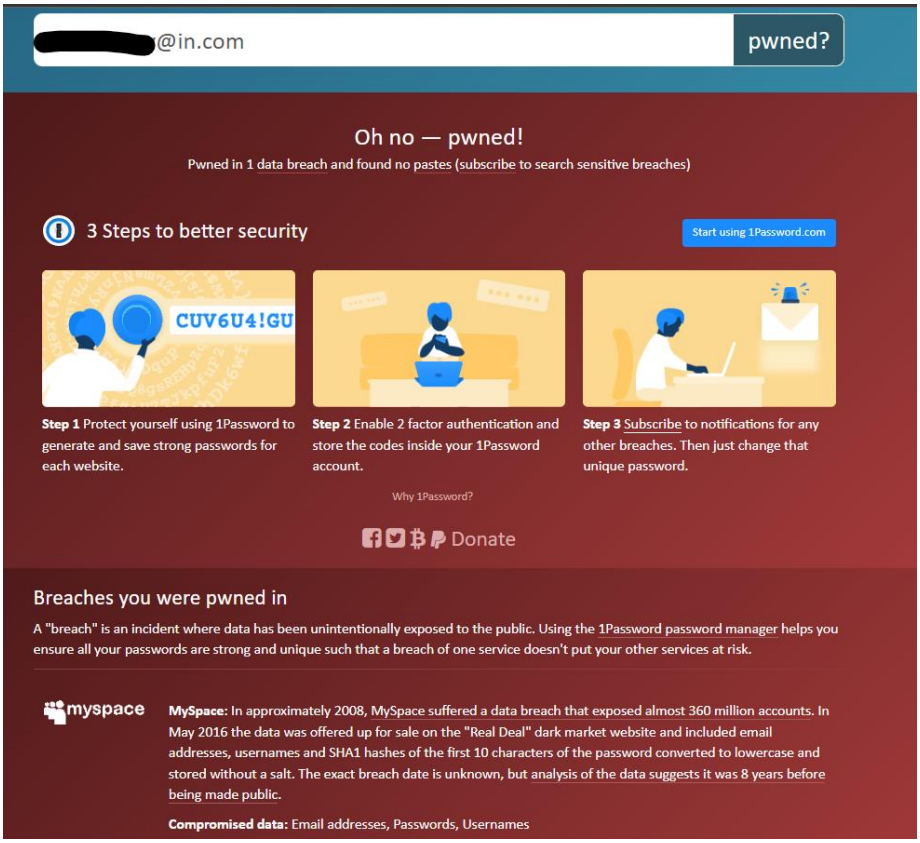
Full information about plans & pricing can be found here: Pricing

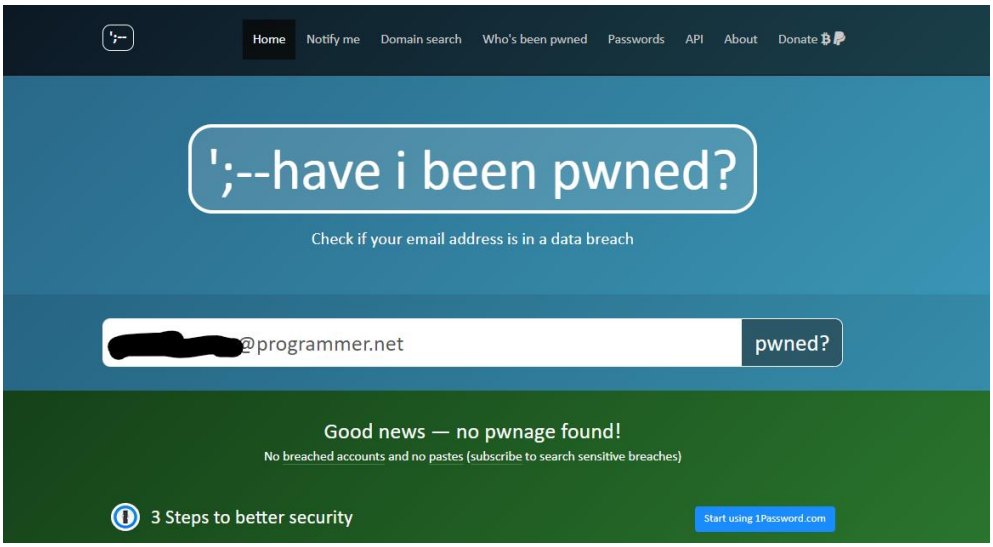
FOCA :
FOCA (Fingerprinting Organizations with Collected Archives) is a network intelligence tool used for analyzing metadata and information leaks in documents. I



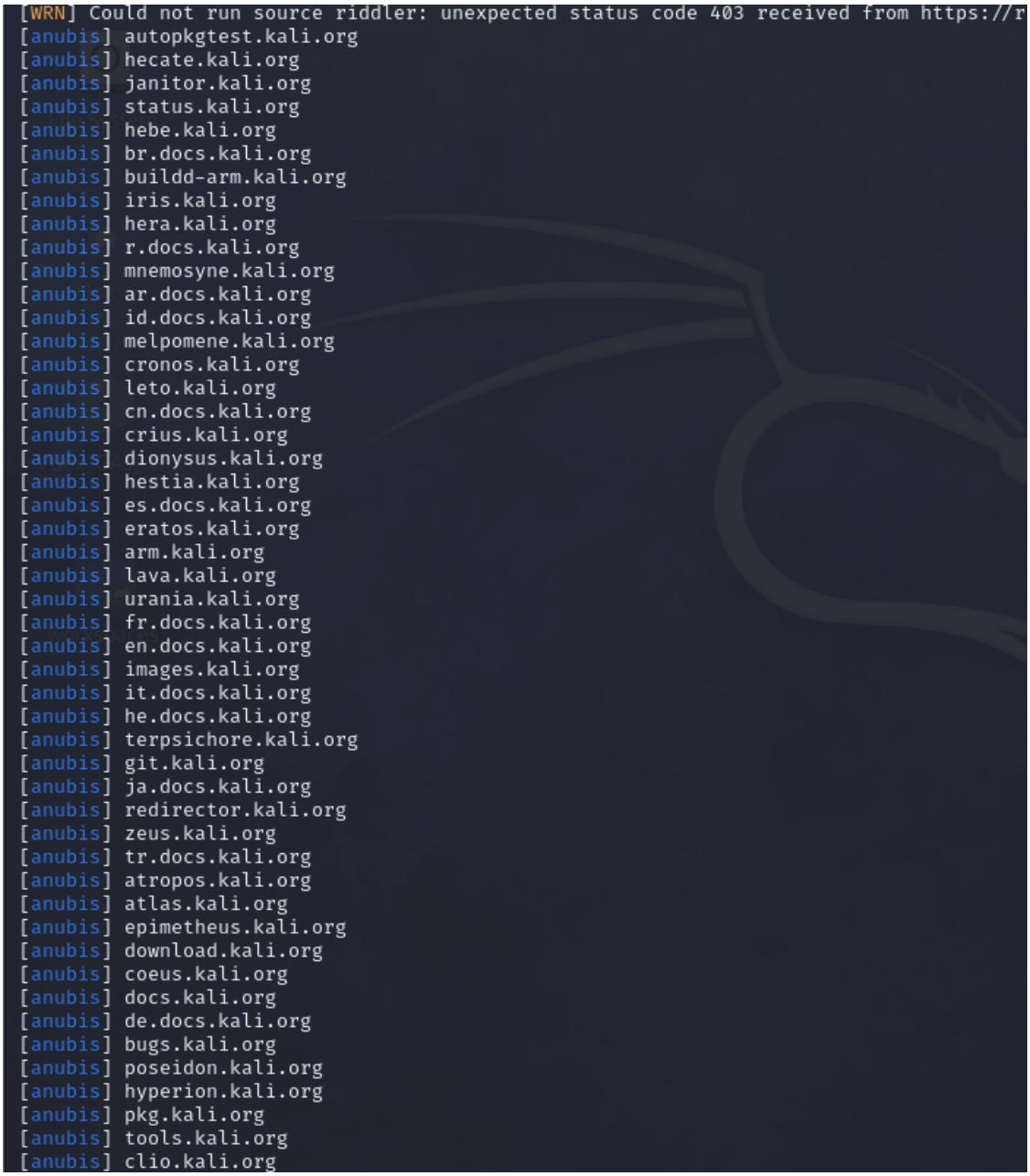


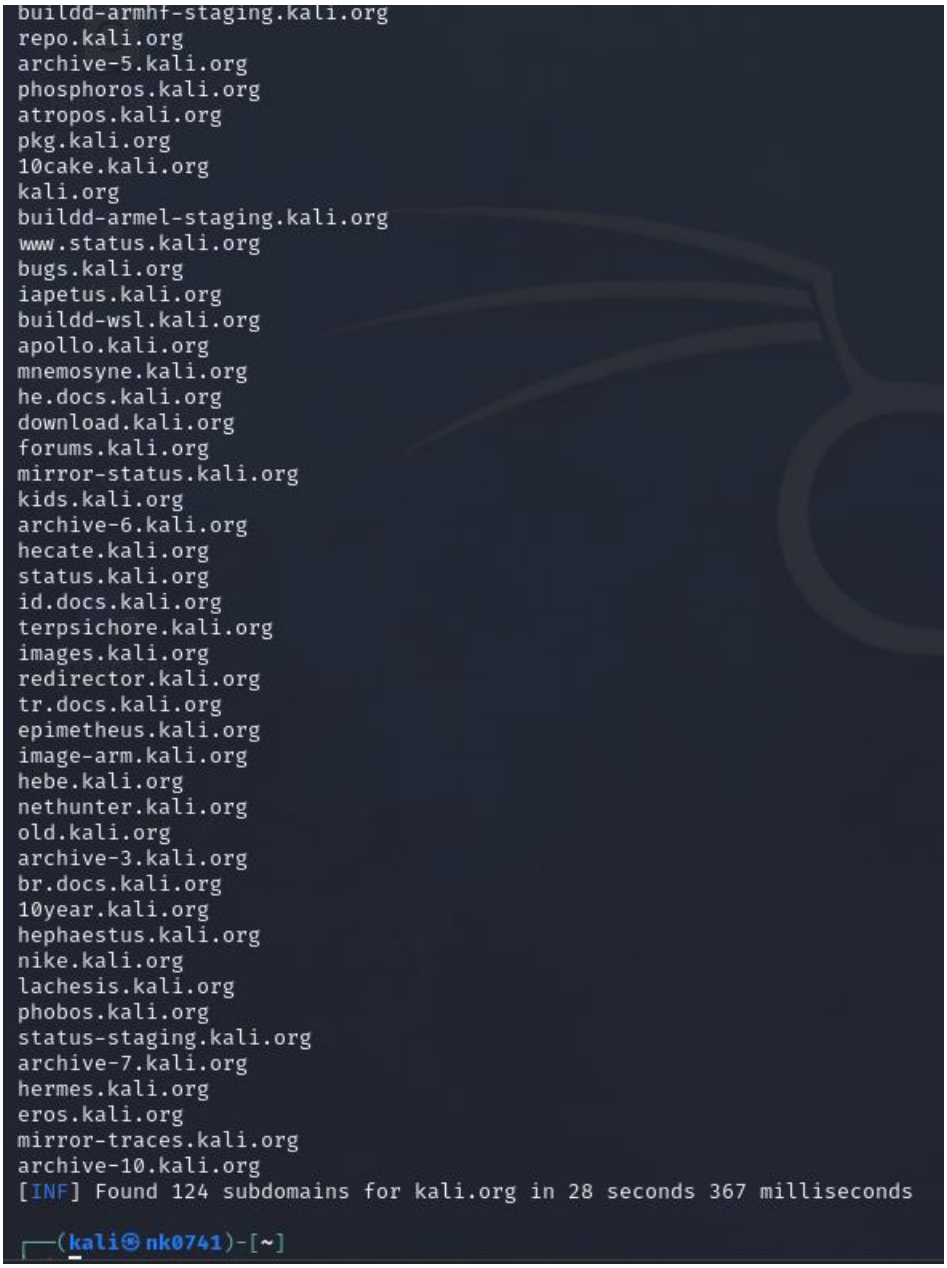
Have I Been Pwned : I used my two different emails to check if there are involved in any data breach or not. Below is the screenshot of the result.



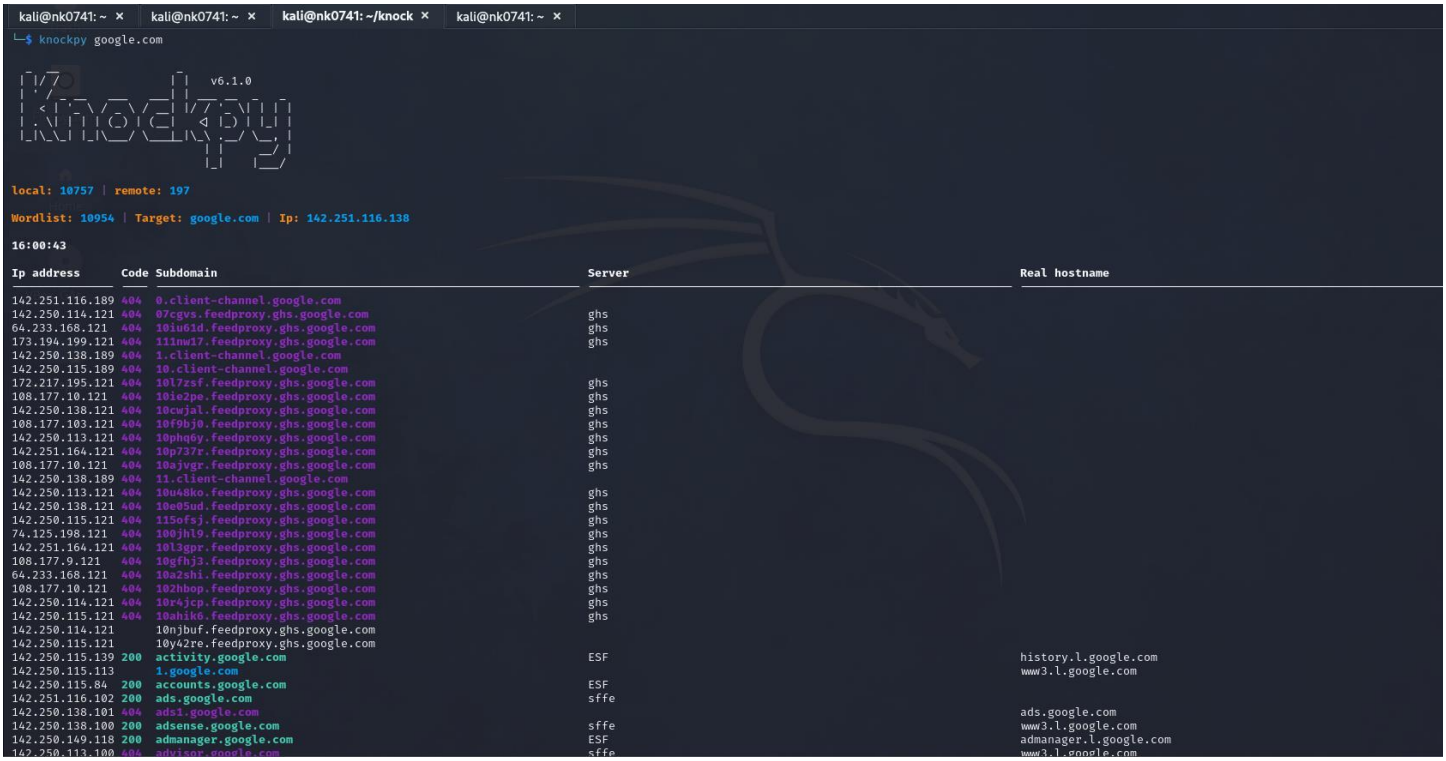


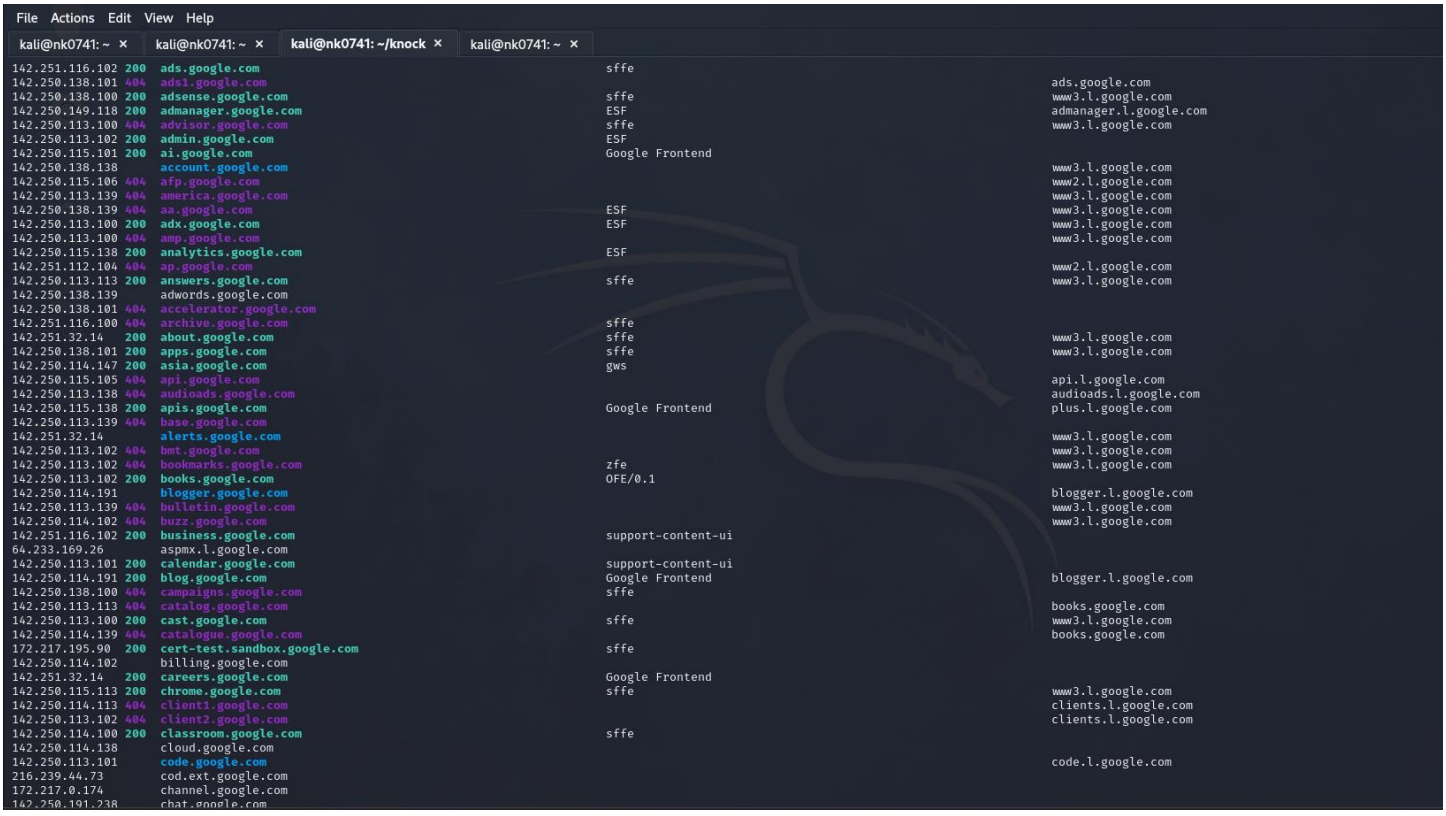
Extra:
SubFinder - Passive: Subfinder is considered a passive open-source intelligence (OSINT) tool used for subdomain discovery


[WRN] Could not run source riddler: unexpected status code 403 received from https://r
[anubis] autopkgtest.kali.org
[anubis] hecate.kali.org
[anubis] janitor.kali.org
[anubis] status.kali.org
[anubis] hebe.kali.org
[anubis] br.docs.kali.org
[anubis] buildd-arm.kali.org
[anubis] iris.kali.org
[anubis] hera.kali.org
[anubis] r.docs.kali.org
[anubis] mnemosyne.kali.org
[anubis] ar.docs.kali.org
[anubis] id.docs.kali.org
[anubis] melpomene.kali.org
[anubis] cronos.kali.org
[anubis] leto.kali.org
[anubis] cn.docs.kali.org
[anubis] crius.kali.org
[anubis] dionysus.kali.org
[anubis] hestia.kali.org
[anubis] es.docs.kali.org
[anubis] eratos.kali.org
[anubis] arm.kali.org
[anubis] lava.kali.org
[anubis] urania.kali.org
[anubis] fr.docs.kali.org
[anubis] en.docs.kali.org
[anubis] images.kali.org
[anubis] it.docs.kali.org
[anubis] he.docs.kali.org
[anubis] terpsichore.kali.org
[anubis] git.kali.org
[anubis] ja.docs.kali.org
[anubis] redirector.kali.org
[anubis] zeus.kali.org
[anubis] tr.docs.kali.org
[anubis] atropos.kali.org
[anubis] atlas.kali.org
[anubis] epimetheus.kali.org
[anubis] download.kali.org
[anubis] coeus.kali.org
[anubis] docs.kali.org
[anubis] de.docs.kali.org
[anubis] bugs.kali.org
[anubis] poseidon.kali.org
[anubis] hyperion.kali.org
[anubis] pkg.kali.org
[anubis] tools.kali.org
[anubis] clio.kali.org

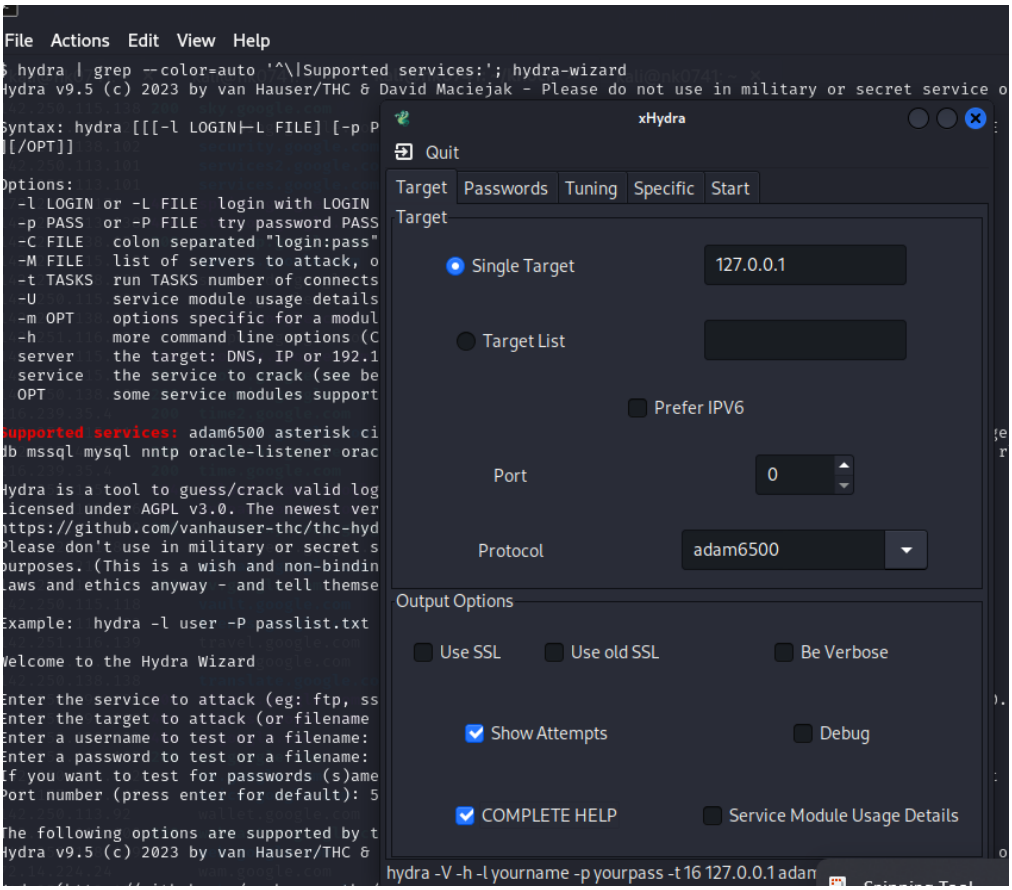


Knockpy- Passive: Knock is an passive tool. It is a Python tool for enumerating subdomains using common techniques like brute-forcing, Google scraping, and certificate transparency.





Hydra-active: Hydra is an active tool in the realm of cybersecurity and open-source intelligence (OSINT). It's a powerful and popular password-cracking tool, often used in penetration testing and security assessments to perform brute force attacks against various protocols such as SSH, FTP, Telnet, HTTP, and others.



Some more tools:

- Sudomy: It is a subdomain enumeration tool written in Python that uses various techniques to discover subdomains.
- Subfinder2: It is an actively maintained fork of the original Subfinder with added features and improvements.
- BeEF: It is an open-source penetration testing tool used to test the security of web browsers. It allows ethical hackers, penetration testers, and security professionals to assess the security posture of a target by exploiting vulnerabilities in the browser.
- Gobuster: It is another popular directory and file brute-forcing tool designed to discover hidden directories and files on web servers. It's written in Go (hence the name) and is known for its speed and efficiency.
- Dirb: It is a popular web application directory brute-forcing tool used for discovering hidden directories and files on a web server. It's written in C and is often included in security testing toolsets due to its efficiency in finding common web application vulnerabilities.

Reference:

https://www.freecodecamp.org/news/an-introduction-to-web-server-scanning-with-nikto/
https://www.geeksforgeeks.org/what-is-sublist3r-and-how-to-use-it/
https://www.youtube.com/watch?v=1AVppUSe7Sk
https://github.com/projectdiscovery/subfinder
https://github.com/guelfoweb/knock
https://medium.com/hacker-toolbelt/knokpy-5c6745e53770
https://www.youtube.com/watch?v=cw59-9s1XhE
https://github.com/vanhauser-thc/thc-hydra
https://github.com/ElevenPaths/FOCA
https://www.youtube.com/watch?v=ieRgYTwxSLA
https://medium.com/@drag0s.stanescu/pdf-metadata-and-practical-examples-of-how-to-handle-it-a6954fa2c374
https://www.hekatron.de/fileadmin/user_upload/testfolder/Sample.pdf

Mitnick, K. (2019). The art of invisibility: The World’s Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data. Back Bay Books.