

Training Report

on

Subdomain Enumeration With Bash Scripting

**Submitted in partial fulfillment of the requirements
for the award of the degree of**

ABSTRACT

The bash script presented herein harnesses the power of three essential cybersecurity tools: Subfinder, gobuster, and assetfinder, to efficiently uncover subdomains associated with a given domain. Designed as a valuable addition to a penetration tester's toolkit, this script streamlines the subdomain discovery process by combining the capabilities of these tools into a single, user-friendly interface.

The script begins by initializing key variables, including the target domain, output directory, wordlist, and optional parameters such as thread count and verbosity. Users are prompted to specify these parameters through command-line arguments.

Following parameter initialization, the script systematically executes subdomain reconnaissance by orchestrating the aforementioned tools. Based on user-specified options, it performs subdomain enumeration using DNS queries, directory brute-forcing, and querying public sources, all while allowing users to customize the level of verbosity and threading to suit their needs.

The script collates the results from these tools, extracts unique subdomains, and saves them into organized text files. Furthermore, it employs httpprobe to identify active subdomains, providing a valuable list of live targets for further assessment.

In summary, this bash script enhances the efficiency and effectiveness of subdomain discovery during security assessments and penetration testing engagements. Its integration of multiple reconnaissance tools simplifies the process, making it a valuable asset for professionals in the field.

List of Figures

Figure No.	Figure Name	Page no.
Figure 4.1	Source Code line 1 to 42	
Figure 4.2	Source Code line 43 to 72	
Figure 4.3	Source Code line 73 to 111	
Figure 4.4	Source Code line 113 to 124	
Figure 6.1	Script Output Screenshots (Subdomains)	
Figure 6.2	Script Generated Files	
Figure 6.3	Probe.txt(Contains all valid subdomains)	

CONTENTS (16 PTS.)

Candidate's Declaration	i
Certificate	ii
Acknowledgement	iii
Abstract	iv
List of Figures	v

CHAPTER NO	DESCRIPTION	PAGE NO.
Chapter 1:	INTRODUCTION	
1.1	What is Subdomain Enumeration?	
1.2	Why is Subdomain Enumeration Important?	
1.3	Challenges in Subdomain Enumeration	
1.4	Subdomain Enumeration and Bash Scripting	
Chapter 2:	Software and Hardware Requirements	
Chapter 3:	Software Requirement Analysis	
3.1	Problem Addressed	
3.2	Modules and Their Functionality	
Chapter 4:	Source Code	
Chapter 5:	Data Flow Diagram	
Chapter 6:	Output Screenshots	
Chapter 7:	Conclusion	
Chapter 8:	References	

1. INTRODUCTION

In the realm of cybersecurity and penetration testing, the pursuit of subdomains stands as a foundational practice for identifying potential entry points and vulnerabilities within a target's digital infrastructure. The process of subdomain enumeration is a crucial precursor to informed security assessments, enabling professionals to uncover hidden assets and assess their security posture.

This report delves into a powerful and streamlined solution for subdomain reconnaissance — a bash script thoughtfully designed to integrate the capabilities of three indispensable tools: dnsrecon, gobuster, and assetfinder. Subdomain enumeration, while a fundamental task, often requires meticulous execution across multiple tools, making it time-consuming and prone to human error. Recognizing this challenge, our script has been developed with the goal of simplifying and enhancing the subdomain discovery process.

Within the following pages, we embark on an exploration of this innovative toolset. We will uncover the intricacies of its design, the mechanics of its execution, and the profound value it brings to the field of cybersecurity. This script is not just a piece of code it's a versatile instrument that empowers cybersecurity professionals to conduct more efficient and effective subdomain reconnaissance.

In this introduction, we set the stage by highlighting the significance of subdomain enumeration in the context of cybersecurity. We will touch upon the challenges faced by professionals in this domain and elucidate the pivotal role that automation plays in mitigating these challenges. Additionally, we will provide an overview of the script's functionality and its relevance within the cybersecurity landscape.

As we proceed, we invite you to journey with us through the intricacies of this bash script, gaining insights into its inner workings, practical applications, and the broader implications it holds for cybersecurity practitioners. Together, we will explore how this tool simplifies and enhances the process of subdomain discovery, ultimately contributing to more informed and effective security assessments.

So, let us begin this exploration, as we unveil a powerful ally in the ever-evolving landscape of cybersecurity: the Bash Subdomain Enumeration Script.

1.1 What is Subdomain Enumeration

Subdomain enumeration is the process of discovering and cataloging subdomains associated with a given domain name. Subdomains are prefixes to the main domain and are used to organize and manage different sections or services of a website or network. Enumerating subdomains is a critical phase in various cybersecurity activities, including penetration testing, vulnerability assessment, and domain management.

There are various subdomain enumeration techniques and tools that one can use to get the desired output. Some of the most common ones are listed below with their corresponding tool for the same.

1. **Brute Force Enumeration:** This technique generates subdomain names by applying dictionaries and checks if they resolve to valid hosts. There are various tools that enable us to perform subdomain enumeration on a target like gobuster, oneforall.py, etc.
2. **DNS Query Enumeration:** In this technique the tools are querying the DNS for subdomains related to a domain, essentially performing a DNS zone transfer. The tools that are famous for this type of subdomain enumeration are dnsrecon, dig, etc.
3. **Certificate Transparency Logs:** Certificate Transparency logs record SSL/TLS certificates issued for subdomains and they might contain a list of subdomains that the certificate is valid for, hence by querying these logs, we can discover subdomains. Some of the tools used for this technique are crt.sh and certspotter.
4. **Web Scraping and Search Engine Queries:** Various search engines index subdomains, so we can extract those subdomains by using web scraping tools for subdomains such as theHarvester, assetfinder, etc.

There are many other types of subdomain enumeration techniques that are being used, but we have mentioned only the most commonly used ones and the ones that will be covered in this project.

1.2 Why is Subdomain Enumeration Important

Subdomain enumeration holds significant importance in the realm of cybersecurity due to its multifaceted role in identifying, assessing, and mitigating potential security risks. First and foremost, subdomains expand the attack surface of a target's digital infrastructure, often serving as overlooked entry points for cyber adversaries. These auxiliary domains can host separate services or resources, each potentially harboring unique vulnerabilities. Therefore, subdomain enumeration plays a pivotal role in vulnerability discovery, enabling security professionals to identify and assess these weaknesses proactively.

Subdomain enumeration aids in early threat detection. By continuously monitoring subdomains, organizations can identify unauthorized or suspicious subdomain creations, serving as a crucial indicator of a security breach or imminent cyberattack. In ethical hacking and penetration testing, this practice is foundational, allowing professionals to simulate real-world attacks, pinpoint weaknesses, and evaluate an organization's overall security posture.

Beyond threat detection, subdomain enumeration contributes to effective asset management. It assists in creating a comprehensive inventory of an organization's digital assets, which is vital for proper asset management and ensuring all assets are adequately protected and monitored. This inventory also feeds into cyber threat intelligence, enabling

security analysts to identify emerging threats, monitor malicious activities, and stay informed about potential risks.

Subdomain enumeration also facilitates attack surface reduction by identifying and managing unnecessary or unused subdomains, thereby minimizing potential entry points for attackers. It also helps in safeguarding against subdomain takeovers, where abandoned or forgotten subdomains become vulnerable to exploitation. By identifying such risks proactively, organizations can prevent subdomain takeover attacks.

Subdomain enumeration assists organizations in adhering to regulatory compliance requirements. Various data protection regulations and standards mandate that organizations maintain an inventory of their digital assets, including subdomains. Compliance with these requirements is simplified through diligent subdomain enumeration practices.

In conclusion, subdomain enumeration serves as a proactive security measure. It empowers organizations to identify and rectify misconfigured or inadequately secured subdomains before they become targets for exploitation. In an ever-evolving threat landscape, subdomain enumeration remains an indispensable practice in fortifying the security and integrity of an organization's online assets and data.

1.3 Challenges in Subdomain Enumeration

Subdomain enumeration, while crucial for cybersecurity, is not without its challenges. One significant challenge is the sheer volume of potential subdomains associated with a domain. Organizations often manage numerous subdomains, making it time-consuming to identify each one manually. Additionally, subdomains may be distributed across multiple DNS servers and cloud services, adding complexity to the enumeration process. Some subdomain names can even be intentionally obfuscated or cryptic, requiring sophisticated dictionary and pattern-based approaches to uncover them. Security measures, such as rate limiting and blocking, imposed by DNS servers can slow down enumeration attempts, making them less effective. The dynamic nature of subdomains, with new ones being created and old ones abandoned, poses another challenge. Lastly, subdomain enumeration may inadvertently raise security alarms, leading to potential IP blocking or detection by intrusion detection systems, necessitating cautious and stealthy enumeration techniques to avoid alerting defenders. Subdomain enumeration presents various obstacles that demand a combination of techniques, tools, and tactics to overcome effectively.

1.4 Subdomain Enumeration and Bash Scripting

In the dynamic landscape of cybersecurity, the practice of subdomain enumeration is indispensable for identifying potential vulnerabilities and entry points within a target's digital infrastructure. However, manually sifting through an extensive list of subdomains can be a time-consuming and error-prone endeavor. This is where the power of bash scripting comes into play, offering a solution that not only reduces effort and time but also enhances the usability and accuracy of results. By crafting bash scripts tailored to the

nuances of subdomain enumeration, security professionals can streamline the entire process. These scripts serve as diligent automatons, executing DNS queries, parsing results, and conducting various enumeration techniques with precision and consistency. The outcome is not just a significant reduction in the human effort required but also an assurance of accuracy, as scripts follow predefined procedures meticulously, eliminating the risk of human errors.

Furthermore, bash scripts bring scalability and thoroughness to the forefront of subdomain enumeration. They can be configured to handle vast volumes of subdomains effortlessly, applying multiple techniques simultaneously or sequentially. This scalability ensures that no subdomain is overlooked, ultimately leading to a more comprehensive assessment of potential vulnerabilities. Importantly, these scripts offer a level of customization that empowers security professionals to adapt their approach to the specific requirements of each assessment. They can choose from a repertoire of subdomain enumeration tools, tailor scanning techniques, and fine-tune parameters to align with the characteristics of the target domain. This adaptability enhances the relevance and efficacy of the enumeration process, as it can be tailored to the unique circumstances of each engagement.

In addition to their automation capabilities, bash scripts incorporate robust error handling and reporting mechanisms. When unforeseen issues such as DNS query failures or rate limiting occur, these scripts are designed to detect, log, and manage errors. They can adjust scanning parameters dynamically and continue execution, minimizing disruptions and enhancing the reliability of the enumeration process. This proactive approach ensures that the enumeration process proceeds smoothly, even in the face of unexpected challenges.

Lastly, well-documented bash scripts serve as valuable assets within cybersecurity teams and organizations. They encapsulate knowledge, best practices, and proven techniques. Sharing these scripts fosters knowledge transfer and accelerates the learning curve for new team members. It also promotes a culture of continuous improvement, as security professionals can build upon and refine existing scripts to adapt to evolving threats and challenges. In summary, the collaboration between bash scripting and subdomain enumeration exemplifies the transformative power of automation in cybersecurity. It empowers professionals to optimize workflows, enhance accuracy, and ultimately secure digital assets more effectively. By reducing the manual effort required while producing usable and accurate results, bash scripts have become an invaluable tool in the arsenal of cybersecurity practitioners striving to stay ahead in the ever-evolving landscape of digital security.

2. Hardware and Software Requirements.

Hardware Requirements:

Minimum

- 2 GB of RAM, 20 GB of storage space.
- At least single-core 64-bit CPU running at 2 GHz or higher.
- Integrated graphics
- HD monitor
- At least 5 Mbps internet connection

Recommended

- 8 GB of RAM, 256 GB of SSD storage
- \geq Intel 13th gen i5 or \geq AMD Ryzen 5 7600x
- AMD Radeon RX 6650 or better Graphics card
- FHD monitor
- 30 Mbps or faster internet connection

Software Requirements:

Operating system

- Kali linux 2023.3 with full dist upgrade

Tools

- Bash
- Ping, Whois, Whatweb, WafW00f, Nmap
- Anew
- Dmitry
- Nslookup
- Gobuster
- Assetfinder
- Subfinder
- Httpprobe
- Aquatone
- Xfce or GNOME desktop environment

3. Software Requirement Analysis

In this section, we delve into the core software-related aspects of our project, aiming to lay the foundation for a clear understanding of our script's purpose, functionality, and architecture.

3.1 Problem Addressed

Our script aims to tackle a fundamental problem in cybersecurity assessments: the need for efficient and accurate subdomain enumeration. Subdomains, while critical for web services and applications, can inadvertently create vulnerabilities if left unmonitored. Therefore, identifying these subdomains efficiently and with precision is vital for early threat detection and comprehensive vulnerability assessment.

Challenges:

1. Automation:

- **Challenge:** Manual subdomain enumeration is a time-consuming and error-prone process, especially when dealing with a substantial number of subdomains.
- **Significance:** The manual approach hinders efficiency, making it impractical for comprehensive assessments.

2. Accuracy:

- **Challenge:** Manual enumeration can lead to inaccuracies and omissions, potentially missing critical subdomains.
- **Significance:** Precision is essential in cybersecurity; missing subdomains could leave vulnerabilities undetected.

3. Time Savings:

- **Challenge:** Manual enumeration is time-consuming, which can be a significant limitation in cybersecurity assessments and investigations.
- **Significance:** In the rapidly evolving cybersecurity landscape, time is of the essence. Delays in identifying subdomains can have serious consequences.

4. Standard Output:

- **Challenge:** Various tools for subdomain enumeration produce output in different format.
- **Significance :** Managing and merging outputs from different tools with diverse formats can be time-consuming and error-prone, especially in time-sensitive cybersecurity assessments. In other words, it can be difficult to understand and merge the outputs of different enumeration tools especially when we are low on time on our hands.

How the script address these problems:

1 .Automation:

- **Efficiency through Automation:** The script automates the entire subdomain enumeration process, eliminating the need for manual, time-consuming efforts. It can handle a substantial number of subdomains efficiently and consistently.
- **Reduced Human Errors:** Automation minimizes the risk of human errors that are inherent in manual enumeration. This ensures the accuracy and completeness of the results.
- **Scalability:** The script is scalable, allowing it to efficiently enumerate subdomains across large target domains. It can tackle comprehensive assessments that would be impractical to perform manually.

2. Accuracy:

- **Comprehensive Enumeration:** By leveraging established subdomain enumeration tools, the script gathers a comprehensive list of subdomains associated with the target domain. It reduces the likelihood of missing critical subdomains.
- **Consistent Methodology:** The script follows a predefined and consistent methodology in subdomain enumeration. This standardization enhances accuracy and ensures that no subdomain is overlooked.
- **Data Integrity:** Post-enumeration, the script processes and consolidates results to maintain data integrity. This reduces inaccuracies that can arise when manually managing multiple sets of data.

3. Time Savings:

- **Rapid Results:** The script significantly reduces the time required for subdomain enumeration. In the swiftly evolving cybersecurity landscape, timely identification of subdomains is essential for staying ahead of potential threats.
- **Resource Optimization:** By automating the enumeration process, the script optimizes resource utilization. Security professionals can focus their time and effort on analyzing results and addressing vulnerabilities rather than manual enumeration tasks.
- **Streamlined Workflow:** Automation streamlines the workflow, reducing delays in identifying subdomains. This is particularly crucial during cybersecurity assessments and investigations, where time-sensitive decisions may need to be made.

4. Standard Output:

- **Output Normalization:** The script incorporates a feature that normalizes the diverse output formats produced by subdomain enumeration tools. It processes and standardizes the results, ensuring a consistent structure.
- **Consolidation:** After standardizing the output, the script combines the results into a single, unified dataset. This consolidation simplifies data management and analysis.
- **Enhanced Readability:** The script generates a clean and easily interpretable output. This enhances the readability of the results and facilitates a more straightforward analysis.

- **Comprehensive Reporting:** The standardized output ensures that all relevant subdomains are presented in a consistent manner, reducing the risk of overlooking critical information.

3.2 Modules and Their Functionality

There are main 9 modules used in this script. Their Basic description and functionality are described below.

- **Ping:** The Linux ping command is a simple utility used to check whether a network is available and if a host is reachable. With this command, you can test if a server is up and running. It also helps with troubleshooting various connectivity issues. Test your internet connection. Check if a remote machine is online.
- **Whois:** WHOIS command is not limited to standard domain or IP address, even we can extract the information of some specific WHOIS server set up by an ICANN. In the below screenshot, we have given the input of the WHOIS Server along with the domain name.
- **Whatweb:** Whatweb offers both passive scanning and aggressive testing. Passive scanning just extracts data from HTTP headers simulating a normal visit. Aggressive options get deeper with recursion & various types of queries & identify all technologies just like a vulnerability scanner.
- **WafW00f:** WAFW00F is a tool that you can use to identify and fingerprints Web Application Firewall (WAF) products. To do its magic, WAFW00F does the following: Sends a normal HTTP request and analyses the response; this identifies a number of WAF solutions.
- **Nmap:** Nmap is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications. Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.

2. Anew:

- **Anew** is a command-line utility designed to manage and ensure the uniqueness of data. In the script, it serves as a data processing tool.
- **Functionality:** Anew takes as input the results from various subdomain enumeration tools, removes duplicate entries, and generates a file containing only unique subdomains. Its purpose is to eliminate redundancy in the subdomain data and create a consolidated list of distinct subdomains for analysis.
- **Significance:** Anew plays a critical role in maintaining data integrity. It ensures that the final subdomain list contains only unique entries, avoiding duplication and inaccuracies that can arise from the output of multiple enumeration tools

3. Dmitry: The dmitry (Deepmagic Information Gathering Tool) tool by James Greig is a command line tool that passively gathers domain registrar information, as well as other public information from web searches (Google) and online statistics sites (Netcraft) about the target systems and creates a log of all information found.

4. Nslookup: Nslookup (stands for “Name Server Lookup”) is a useful command for getting information from the DNS server. It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record. It is also used to troubleshoot DNS-related problems.

5. Gobuster:

- **Gobuster** is a specialized directory and file brute-forcing tool used in web application security testing. Within the script, it functions as a directory enumeration tool.
- **Functionality:** Gobuster systematically scans the target domain for common directories and paths, providing information about accessible web resources. Its role is to identify potential web assets and paths on the target domain.
- **Significance:** Gobuster enhances the script's ability to map out the web infrastructure of the target domain. It identifies directories and paths that could be potential entry points, aiding in vulnerability assessment and penetration testing.

6. Assetfinder:

- **Assetfinder** is a subdomain discovery tool designed to find and extract subdomains associated with a given domain. In the script, it serves as a subdomain enumeration tool.
- **Functionality:** Assetfinder queries public sources and DNS records to identify subdomains exclusively. Its purpose is to compile a list of subdomains associated with the target domain.
- **Significance:** Assetfinder broadens the scope of subdomain enumeration. It leverages external sources and DNS records to uncover subdomains that may not be visible through traditional means, providing a comprehensive subdomain dataset.

7. Subfinder: subfinder is a subdomain discovery tool that discovers valid subdomains for websites by using passive online sources. It has a simple modular architecture and is optimized for speed. subfinder is built for doing one thing only – passive subdomain enumeration, and it does that very well.

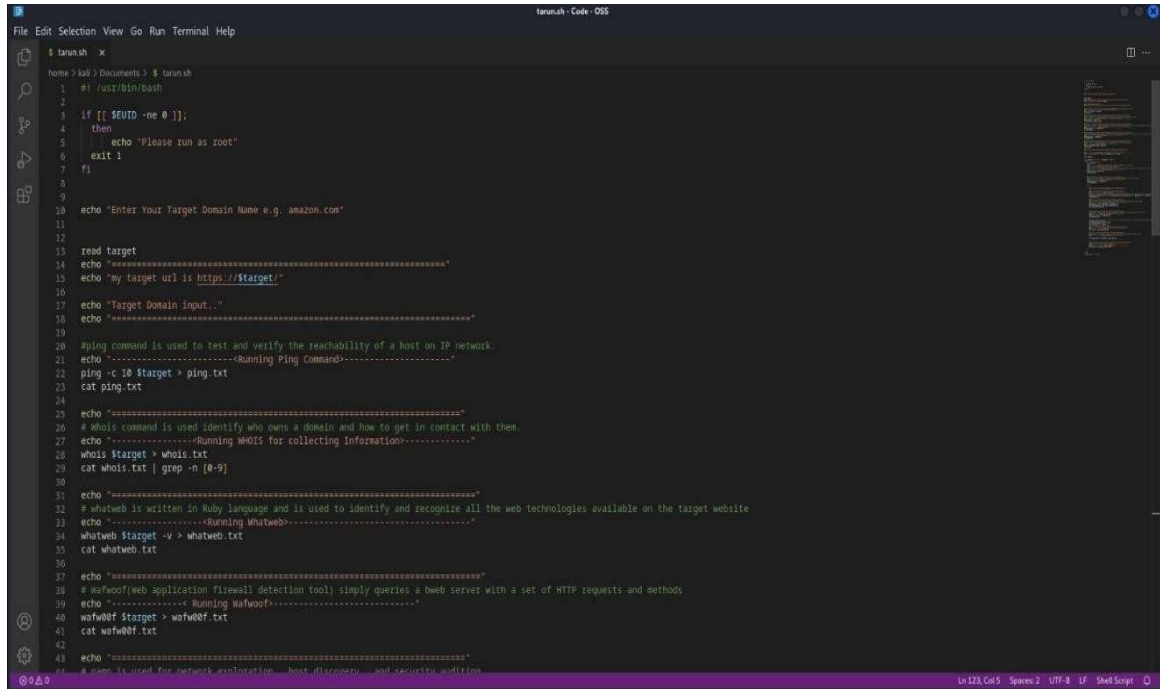
8. Httpprobe:

- **Httpprobe** is a tool used to verify the accessibility and validity of web resources. Within the script, it functions as a subdomain validation tool.

- **Functionality:** Httpprobe tests each discovered subdomain to determine if it is active and reachable via HTTP or HTTPS. It plays a crucial role in identifying working and valid subdomains, essential for further analysis.
- **Significance:** Httpprobe ensures that the subdomains identified are not only present but also active. It helps in distinguishing between dormant subdomains and those that could pose a real security risk.

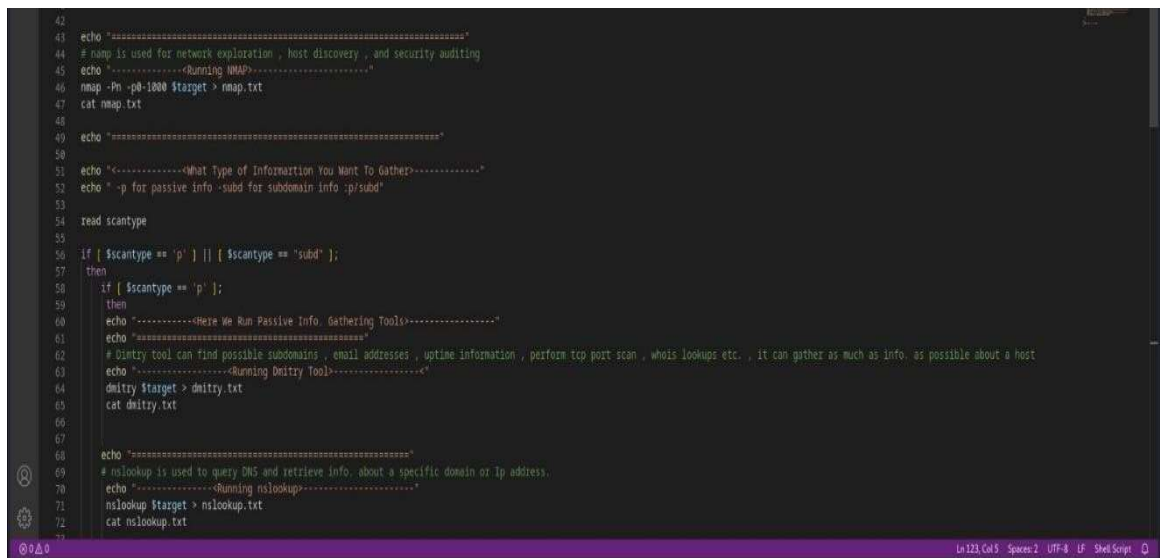
4. Source Code

This chapter contains the source code for the bash script that does automatic subdomain enumerations and gives us a standard output in a text file. The text file contains all the working subdomains and all the entries of the file are unique.



```
1 #!/usr/bin/bash
2
3 if [[ $UID -ne 0 ]];
4 then
5     echo "Please run as root"
6     exit 1
7 fi
8
9
10 echo "Enter Your Target Domain Name e.g. amazon.com"
11
12
13 read target
14 echo "=====
15 echo "my target url is https://$target/"
16
17 echo "Target Domain Input.."
18 echo "=====
19
20 #ping command is used to test and verify the reachability of a host on IP network.
21 echo "-----Running Ping Command-----"
22 ping -c 10 $target > ping.txt
23 cat ping.txt
24
25 echo "=====
26 # whois command is used to identify who owns a domain and how to get in contact with them.
27 echo "-----Running WHOIS for collecting Information-----"
28 whois $target > whois.txt
29 cat whois.txt | grep -n [0-9]
30
31 echo "=====
32 # whatweb is written in Ruby language and is used to identify and recognize all the web technologies available on the target website
33 echo "-----Running whatweb-----"
34 whatweb $target -v > whatweb.txt
35 cat whatweb.txt
36
37 echo "=====
38 # wafw00f (web application firewall detection tool) simply queries a web server with a set of HTTP requests and methods
39 echo "-----Running wafw00f-----"
40 wafw00f $target > wafw00f.txt
41 cat wafw00f.txt
42
43 echo "=====
44 # nmap is used for network exploration , host discovery , and security auditing
```

Figure 4.1: Source code line 1 to 42



```
43 echo "=====
44 # nmap is used for network exploration , host discovery , and security auditing
45 echo "-----Running NMAP-----"
46 nmap -Pn -p0-1000 $target > nmap.txt
47 cat nmap.txt
48
49 echo "=====
50
51 echo "-----What Type of Information You Want To Gather-----"
52 echo " -p for passive info -subd for subdomain info :p/subd"
53
54 read scantype
55
56 if [ $scantype == 'p' ] || [ $scantype == 'subd' ];
57 then
58     if [ $scantype == 'p' ];
59     then
60         echo "-----Here We Run Passive Info. Gathering Tools-----"
61         echo "=====
62         # dmitry tool can find possible subdomains , email addresses , uptime information , perform tcp port scan , whois lookups etc. , it can gather as much as info. as possible about a host
63         echo "-----Running Dmitry Tool-----"
64         dmitry $target > dmitry.txt
65         cat dmitry.txt
66
67         echo "=====
68         # nslookup is used to query DNS and retrieve info. about a specific domain or Ip address.
69         echo "-----Running nslookup-----"
70         nslookup $target > nslookup.txt
71         cat nslookup.txt
72
73         echo "=====
```

Figure 4.2: Source code line 43 to 72

```

74 else
75
76     echo " Here We Are Running SubDomains Info. Gathering Tools..."
77
78     echo "=====Running Gobuster=====
79     echo "-----Running Gobuster-----"
80     # gobuster enumerates hidden directories and files in the target domain by performing a brute force attack
81     gobuster dns -d $target -t 10 -w /usr/share/wordlists/dirb/common.txt -qz > gobuster.txt -i --wloccard
82     cat gobuster.txt
83
84     echo "=====Running assetfinder=====
85     #assetfinder is used to find domains and subdomains potentially related to a given domain
86     echo "-----Running assetfinder-----"
87     assetfinder --subs-only $target > assetfinder.txt
88     cat assetfinder.txt | anew sorts_assetfinder.txt
89     cat sorts_assetfinder.txt
90
91
92     echo "=====Running subfinder=====
93     # subfinder is used to discover valid subdomains for websites by using passive online sources.
94     echo "-----Running subfinder-----"
95     subfinder -d $target > subfinder.txt
96     cat subfinder.txt
97
98     # here , we concatenate all our outputs of .txt files and stores them in ore specified directory(results)
99     cat gobuster.txt >> results
100    cat sorts_assetfinder.txt >> results
101    cat subfinder.txt >> results
102    # anew is used to sort the outputs
103    echo "=====Running anew=====
104    echo "-----Running anew-----"
105    cat results | anew unique_results
106
107    echo "=====Running httpprobe=====
108    #httpprobe is a tool which is used for quickly probing for active http and http servers
109    echo "-----Starting Httpprobe-----"
110
111    cat unique_results | httpprobe | anew probe.txt
112
113

```

Figure 4.3: Source code line 73 to 111

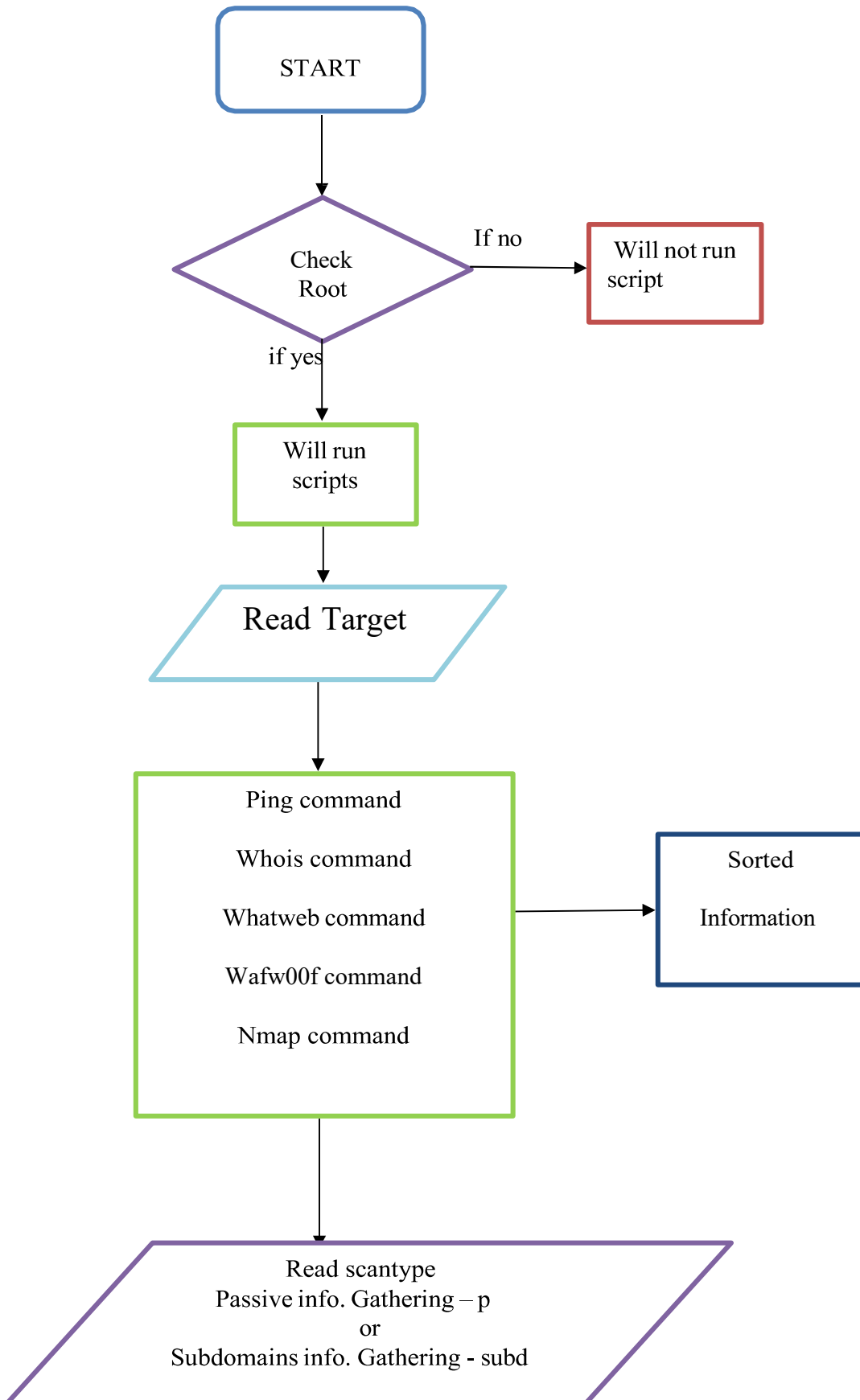
```

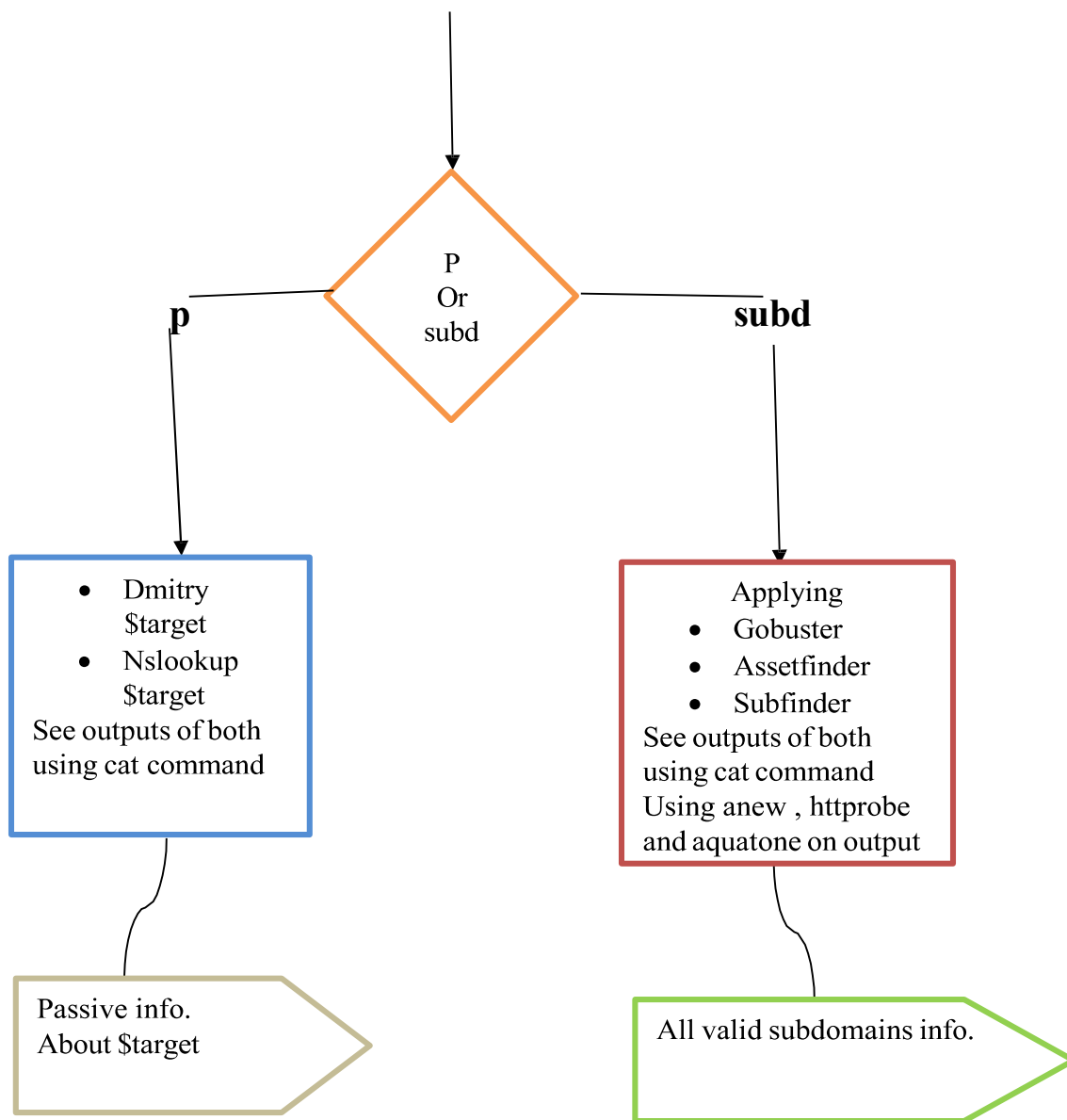
112
113
114    echo "=====Running Aquatone=====
115    #Aquatone tool is used to take screenshots
116    echo "-----Running Aquatone-----"
117    cat probe.txt | aquatone -ports large
118
119    fi
120
121    else
122        echo "enter p or subd.."
123    fi
124

```

Figure 4.4: Source code line 112 to 124

5. Data Flow Diagram





6. Output Screenshots

This chapter contains all the output screenshots for the domain ‘google.com and Instagram.com’.

Here, First we do passive information gathering of ‘google.com’, after that, we will find subdomains of any other website ‘Instagram.com’

Passive Information of Website ‘Google.com’

Here, we have to run our scripts in root terminal. If not root, then it will not run.

```
root@kali: ~/Documents
File Actions Edit View Help

kali@kali:~$ cd Documents
kali@kali:~/Documents$ ./tarun.sh
Please run as root

root@kali:~/Documents$ ./tarun.sh
Enter Your Target Domain Name e.g. amazon.com
google.com

my target url is https://google.com/
Target Domain input..

--Running Ping Command--
PING google.com (142.250.193.46) 56(84) bytes of data:
64 bytes from del11s15-in-f14.1e100.net (142.250.193.46): icmp_seq=1 ttl=57 time=15.9 ms
64 bytes from del11s15-in-f14.1e100.net (142.250.193.46): icmp_seq=2 ttl=57 time=18.4 ms
64 bytes from del11s15-in-f14.1e100.net (142.250.193.46): icmp_seq=3 ttl=57 time=96.0 ms
64 bytes from del11s15-in-f14.1e100.net (142.250.193.46): icmp_seq=4 ttl=57 time=27.5 ms
64 bytes from del11s15-in-f14.1e100.net (142.250.193.46): icmp_seq=5 ttl=57 time=32.5 ms
64 bytes from del11s15-in-f14.1e100.net (142.250.193.46): icmp_seq=6 ttl=57 time=32.7 ms
64 bytes from del11s15-in-f14.1e100.net (142.250.193.46): icmp_seq=7 ttl=57 time=51.9 ms
64 bytes from del11s15-in-f14.1e100.net (142.250.193.46): icmp_seq=8 ttl=57 time=48.7 ms
64 bytes from del11s15-in-f14.1e100.net (142.250.193.46): icmp_seq=9 ttl=57 time=45.3 ms
64 bytes from del11s15-in-f14.1e100.net (142.250.193.46): icmp_seq=10 ttl=57 time=52.5 ms

-- google.com ping statistics --
10 packets transmitted, 10 received, 0% packet loss, time 9014ms
rtt min/avg/max/ndev = 15.891/47.322/96.035/21.947 ms

--Running WHOIS for collecting Information--
getaddrinfo(whois.markmonitor.com): Temporary failure in name resolution
2: Registry Domain ID: 2138514_DOMAIN_COM-VRSN
5: Updated Date: 2019-09-09T15:19:04Z
6: Creation Date: 1997-09-15T04:00:00Z
7: Registry Expiry Date: 2028-09-14T04:00:00Z
9: Registrar IANA ID: 292
11: Registrar Abuse Contact Phone: +1.206.665.1750
18: Name Server: NS1.GOOGLE.COM
19: Name Server: NS2.GOOGLE.COM
20: Name Server: NS3.GOOGLE.COM
21: Name Server: NS4.GOOGLE.COM
24: Last update of whois database: 2023-09-12T04:33:25Z ok
45: (1) allow, enable, or otherwise support the transmission of mass
47: (1) allow, enable, or otherwise support the transmission of mass
47: (2) enable high volume, automated, electronic processes
```

```
File Actions Edit View Help
--(Running Whatweb)--
WhatWeb report for http://google.com
Status : 301 Moved Permanently
Title : 301 Moved
IP : 142.250.193.78
Country : UNITED STATES, US

Summary : HTTPServer[gs], RedirectLocation[http://www.google.com/], UncommonHeaders[content-security-policy-report-only], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[0]

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

    String : gs (from server string)

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

    String : http://www.google.com/ (from location)

[ 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 : content-security-policy-report-only (from headers)

[ 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 : 0

HTTP Headers:
HTTP/1.1 301 Moved Permanently
Location: http://www.google.com/
Content-Type: text/html; charset=UTF-8
Content-Security-Policy-Report-Only: object-src 'none' base-uri 'self'; script-src 'nonce-SjVSegeKJlVHCYCo5gBQ' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https://report-uri https://csp.withgoogle.com/csp/gws/other-hp
Date: Tue, 12 Sep 2023 04:33:59 GMT
Expires: Thu, 12 Oct 2023 04:33:59 GMT

csp/gws/other-hp
Date: Tue, 12 Sep 2023 04:33:59 GMT
Expires: Thu, 12 Oct 2023 04:33:59 GMT
Cache-Control: public, max-age=2592000
Server: gs
Content-Length: 219
X-XSS-Protection: 0
X-Frame-Options: SAMEORIGIN
Connection: close

WhatWeb report for http://www.google.com/
Status : 200 OK
Title : Google
IP : 142.251.42.36
Country : UNITED STATES, US

Summary : Cookies[IP,AR,AC,NID], HTML5, HTTPServer[gs], HttpOnly[AEC,NID], Script, UncommonHeaders[content-security-policy-report-only], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[0]

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

    String : IP_3AN
    String : AR
    String : NID

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

[ HTTPServer ]
    HTTP server header string. This plugin also attempts to
```

```

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

  String      : gws (from server string)

[ HttpOnly ]
  If the HttpOnly flag is included in the HTTP set-cookie
  response header and the browser supports it then the cookie
  cannot be accessed through client side script - More Info:
  http://en.wikipedia.org/wiki/HTTP_cookie

  String      : ALC, NID

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

[ 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. expires-by, server and x-aspnet-version.
  Info about headers can be found at www.http-stats.com

  String      : content-security-policy-report-only (from headers)

[ 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      : 0

```

```

HTTP Headers:
  HTTP/1.1 200 OK
  Date: Tue, 12 Sep 2023 04:34:00 GMT
  Expires: -1
  Cache-Control: private, max-age=0
  Content-Type: text/html; charset=ISO-8859-1

```

root@kali: ~/Documents

File Actions Edit View Help

Set-Cookie: NID=511=mvh05jhdwsew_sawtzgziqf18yGfFCsInCPabJBoIXEvFhd_dvb7xXcEhscN0053MzpyUNP7IOVAATu_QM3Aa2m5g2035m0u5a38ah42MRkMl.qzSq[7]JMKrg3ZEK2ESTNRFS9D1bA9HEV0735jq2IV08mJyVFN10; expires=Wed, 13-Mar-2024 04:34:00 GMT; path=/; domain=.google.com; HttpOnly
 Connection: close

Running Nmap

404 Not Found

405 Not Allowed

403 Forbidden

502 Bad Gateway

500 Internal Error

Running Nmap

Starting Nmap 7.94 (https://nmap.org) at 2023-09-12 00:34 EDT
 Nmap scan report for google.com (142.250.193.78)
 Host is up (0.003s latency).
 Other addresses for google.com (not scanned): 2404:6808:4002:81a::200e
 rDNS record for 142.250.193.78: dellis16-in-f14.1e100.net
 Not shown: 998 filtered tcp ports (no-response), 1 filtered tcp ports (net-unreach)
 PORT STATE SERVICE
 80/tcp open http
 443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 0.62 seconds

```
ret@kali: /home/ret/Documents
File Actions Edit View Help
-----
<Here We Run Passive Info. Gathering Tools>
-----
<Running Dnifly Tool>
-----
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:142.250.193.46
HostName:google.com

Gathered Inet-whois information for 142.250.193.46

inetnum:      142.248.0.0 - 142.248.255.255
netname:      NW-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 Caribbean)
remarks:      http://www.lacnic.net/ whois.lacnic.net
remarks:
country:      EU # Country is really world wide
admin-c:      IANA1-RIPE
tech-c:        IANA1-RIPE
status:        ALLOCATED UNSPECIFIED
mnt-by:        RIPE-NCC-MNT
created:        2023-07-27T14:32:14Z
last-modified:  2023-07-24T14:32:14Z
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 1.107 (ABOIDEEN)

Gathered Inic-whois information for google.com

Domain Name: GOOGLE.COM
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:39:04Z
Creation Date: 1997-09-15T04:00:00Z
Registry Expiry Date: 2020-09-14T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2089851750
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: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
DNSSEC: unsigned
URL of the IANA Whois Repository: http://www.iana.org/whois
```

Gathered Netcraft information for google.com

Retrieving Netcraft.com information for google.com
Netcraft.com Information gathered

Gathered Subdomain information for google.com

Searching Google.com:80 ...
HostName:www.google.com
HostIP:142.250.183.196
Searching Altavista.com:80 ...
Found 1 possible subdomain(s) for host google.com, Searched 0 pages containing 0 results

Gathered E-Mail information for google.com

Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 E-Mail(s) for host google.com, Searched 0 pages containing 0 results

Gathered TCP Port information for 142.250.193.46

Port	State
------	-------

80/tcp	open
--------	------

Portscan Finished: Scanned 150 ports, 0 ports were in state closed

All scans completed, exiting

(Running nslookup)

Server: 8.8.8.8
Address: 8.8.8.8953

Non-authoritative answer:

Name: google.com
Address: 142.250.193.46
Name: google.com
Address: 2404:6800:4002:61a::200e

Subdomains information Gathering of Website ‘Instagram.com’

```
File Actions Edit View Help

root@kali: ~/home/kali/Documents

--(What Type of Information You Want To Gather)--
-p for passive info -subd for subdomain info :p/subd
subd
Here We Are Running SubDomains Info. Gathering Tools....

--(Running GOBuster)--
Found: about.instagram.com [157.240.198.17,2a03:2880:f044:12:face:b00c:0:2]
Found: About.instagram.com [157.240.198.17,2a03:2880:f044:12:face:b00c:0:2]
Found: Admin.instagram.com [157.240.198.8,2a03:2880:f044:8:face:b00c:0:2]
Found: admin.instagram.com [157.240.198.8,2a03:2880:f044:8:face:b00c:0:2]
Found: ADMIN.instagram.com [157.240.198.8,2a03:2880:f044:8:face:b00c:0:2]
Found: api.instagram.com [157.240.198.63,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: auth.instagram.com [157.240.198.63,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: autodiscover.instagram.com [62.96.57.168,52.96.123.216,40.99.33.246,52.98.123.232,2003:1046:c04:1018::8,2003:1046:c04:800::8,2003:1046:c04:818::8,2003:1046:c04:1019::8]
Found: black.instagram.com [157.240.198.63,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: blog.instagram.com [157.240.198.17,2a03:2880:f044:12:face:b00c:0:2]
Found: Blog.instagram.com [157.240.198.17,2a03:2880:f044:12:face:b00c:0:2]
Found: brand.instagram.com [157.240.198.17,2a03:2880:f044:12:face:b00c:0:2]
Found: business.instagram.com [157.240.198.63,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: Business.instagram.com [157.240.198.63,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: call.instagram.com [157.240.198.63,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: checkout.instagram.com [157.240.198.63,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: community.instagram.com [157.240.198.63,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: developers.instagram.com [157.240.198.17,2a03:2880:f044:12:face:b00c:0:2]
Found: employee.instagram.com [18.118.136.2,2a01:d00:21ff:6:face:b00c:0:5722]
Found: survey.instagram.com [157.240.198.63,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: threads.instagram.com [157.240.198.63,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: upload.instagram.com [157.240.198.63,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: white.instagram.com [157.240.198.63,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: www.instagram.com [157.240.198.174,2a03:2880:f244:e0:face:b00c:0:4420]

--(Running assetfinder)--
instagram.com
support-instagram.com
l.instagram.com
platform.instagram.com
www.instagram.com
instagram.cldr.instagram.com
2-p42-instagram.cldr.instagram.com
a.es.instagram.com
b.es.instagram.com
c.es.instagram.com
d.es.instagram.com
j.instagram.com
latest.instagram.com
maps.instagram.com
trunktable.instagram.com
intern.instagram.com
secure.latest.instagram.com
cdninstagram.com
*.instagram.com
graph.instagram.com
prod.instagram.com
m.instagram.com
beta.instagram.com

www.mail--instagram.com
unknownjapan.instagram.com
engineering.instagram.com
www.engineering.instagram.com
partners.business.instagram.com
api.instagram.com
instagram.com
support-instagram.com
l.instagram.com
platform.instagram.com
www.instagram.com
instagram.cldr.instagram.com
2-p42-instagram.cldr.instagram.com
a.es.instagram.com
b.es.instagram.com
c.es.instagram.com
d.es.instagram.com
j.instagram.com
latest.instagram.com
maps.instagram.com
trunktable.instagram.com
intern.instagram.com
secure.latest.instagram.com
cdninstagram.com
*.instagram.com
graph.instagram.com
prod.instagram.com
m.instagram.com
beta.instagram.com
upload.instagram.com
secure.instagram.com
autodiscover.instagram.com
graphl.instagram.com
copyright--instagram.com
www.copyright--instagram.com
cpanel.security--instagram.com
cpalendars.security--instagram.com
cpcontacts.security--instagram.com
mail.security--instagram.com
security--instagram.com
webdisk.security--instagram.com
webmail.security--instagram.com
www.security--instagram.com
mail--instagram.com
cpanel.mail--instagram.com
mail.mail--instagram.com
webdisk.mail--instagram.com
webmail.mail--instagram.com
www.mail--instagram.com
unknownjapan.instagram.com
engineering.instagram.com
www.engineering.instagram.com
partners.business.instagram.com
api.instagram.com
```



```
root@kali: /home/kali/Documents
File Actions Edit View Help
Running Subfinder

projectdiscovery.io

[WARN] Use with caution. You are responsible for your actions.
[WARN] Developers assume no liability and are not responsible for any misuse or damage.
[WARN] By using subfinder, you also agree to the terms of the APIs used.

[100] Enumerating subdomains for instagram.com
api.instagram.com
autodiscover.instagram.com
beta.instagram.com
engineering.instagram.com
graph.instagram.com
i.instagram.com
instagram.com
intern.instagram.com
latest.instagram.com
maps.instagram.com
m.instagram.com
partners.business.instagram.com
platform.instagram.com
prod.instagram.com
secure.instagram.com
secure.latest.instagram.com
trunkstable.instagram.com
unknownjapan.instagram.com
upload.instagram.com
www.engineering.instagram.com
www.instagram.com
badges.instagram.com
blog.instagram.com
business.instagram.com
demo.instagram.com
distilleryimage0.ak.instagram.com
distilleryimage0.instagram.com
distilleryimage1.ak.instagram.com
distilleryimage1.instagram.com
distilleryimage10.ak.instagram.com
distilleryimage10.instagram.com
distilleryimage11.ak.instagram.com
distilleryimage11.instagram.com
distilleryimage2.ak.instagram.com
distilleryimage2.instagram.com
distilleryimage3.ak.instagram.com
distilleryimage3.instagram.com
distilleryimage4.ak.instagram.com
distilleryimage4.instagram.com
distilleryimage5.ak.instagram.com
distilleryimage5.instagram.com
distilleryimage6.ak.instagram.com
distilleryimage6.instagram.com
distilleryimage7.ak.instagram.com
distilleryimage7.instagram.com
distilleryimage8.ak.instagram.com
distilleryimage8.instagram.com
distilleryimage9.ak.instagram.com
distilleryimage9.instagram.com
distilleryvesperi-1.ak.instagram.com
distilleryvesperi-5.ak.instagram.com
distilleryvesperi10-6.ak.instagram.com
distilleryvesperi11.ak.instagram.com
distilleryvesperi15.ak.instagram.com
distilleryvesperi2-10.ak.instagram.com
distilleryvesperi2-2.ak.instagram.com
distilleryvesperi3-10.ak.instagram.com
distilleryvesperi4-8.ak.instagram.com
distilleryvesperi5-13.ak.instagram.com
distilleryvesperi5-17.ak.instagram.com
distilleryvesperi5-9.ak.instagram.com
distilleryvesperi7-11.ak.instagram.com
distilleryvesperi7-19.ak.instagram.com
distilleryvesperi7-7.ak.instagram.com
distilleryvesperi8-12.ak.instagram.com
distilleryvesperi8-4.ak.instagram.com
distilleryvesperi8-8.ak.instagram.com
distilleryvesperi9-13.ak.instagram.com
distilleryvesperi9-5.ak.instagram.com
distilleryvesperi9-9.ak.instagram.com
grammys.instagram.com
```

```
File Actions Edit View Help
default-geo.instagram.com
developers.instagram.com
z-p4-ww.instagram.com
z-p42.graph.instagram.com
z-p4.l.instagram.com
edge-chat.instagram.com
d.ms.instagram.com
mail.instagram.com
my-od-5.instagram.com
my-od-2.instagram.com
my-od-4.instagram.com
my-od-1.instagram.com
web.instagram.com
auth.instagram.com
privacycenter.instagram.com
pandemic105.latest.instagram.com
en-gb.latest.instagram.com
help.hyperlane.beta.latest.instagram.com
z-p15.l.instagram.com
www.intern.instagram.com
employee.instagram.com
z-p4.upload.instagram.com
safety.instagram.com
beta.latest.instagram.com
developers.latest.instagram.com
survey.instagram.com
z-p15.graph.instagram.com
z-p42.dyn.www.instagram.com
black.instagram.com
z-p42.maps.instagram.com
instagram-ww.instagram.com
graph-fallback.instagram.com
star.fallback.clor.instagram.com
creators.instagram.com
lww.instagram.com
twbared2589.11.vlll.instagram.com
xm-ww-8463bya.instagram.com
i.secure.instagram.com
familycenter.instagram.com
i.b.instagram.com
wallets.instagram.com
white.ish.instagram.com
black.ish.instagram.com
ish.instagram.com
p.instagram.com
od.instagram.com
www.hlp.instagram.com
downtumbre.instagram.com
9387adbf41d.instagram.com
www.l.instagram.com
e213f691ec9f.instagram.com
instagram.clor.facebook.comww.instagram.com
star-mini.clor.facebook.comww.instagram.com
chat.instagram.com
2fbusiness.instagram.com
iness.instagram.com

-----
--(Running anew)--
Found: about.instagram.com [157.240.198.17,2a03:2880:f044:12:face:b00c:0:2]
Found: About.instagram.com [157.240.198.17,2a03:2880:f044:12:face:b00c:0:2]
Found: Admin.instagram.com [157.240.198.8,2a03:2880:f044:18:face:b00c:0:420d]
Found: admin.instagram.com [157.240.198.8,2a03:2880:f044:18:face:b00c:0:420d]
Found: ADMIN.instagram.com [157.240.198.8,2a03:2880:f044:18:face:b00c:0:420d]
Found: api.instagram.com [157.240.198.63,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: auth.instagram.com [157.240.198.63,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: autodiscover.instagram.com [52.96.57.168,52.96.123.216,40.99.33.240,52.96.123.232,2603:1046:c04:1018::8,2603:1046:c04:1019::8,2603:1046:c04:1018::8,2603:1046:c04:1019::8]
Found: black.instagram.com [157.240.198.62,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: blog.instagram.com [157.240.198.17,2a03:2880:f044:12:face:b00c:0:2]
Found: Blog.instagram.com [157.240.198.17,2a03:2880:f044:12:face:b00c:0:2]
Found: brand.instagram.com [157.240.198.17,2a03:2880:f044:12:face:b00c:0:2]
Found: business.instagram.com [157.240.198.63,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: Business.instagram.com [157.240.198.63,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: call.instagram.com [157.240.198.63,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: checkout.instagram.com [157.240.198.63,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: community.instagram.com [157.240.198.63,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: developers.instagram.com [157.240.198.27,2a03:2880:f044:12:face:b00c:0:2]
Found: employee.instagram.com [10.110.136.2,2a03:d000:21ff:6:face:b00c:0:5722]
Found: survey.instagram.com [157.240.198.63,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: threads.instagram.com [157.240.198.63,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: upload.instagram.com [157.240.198.63,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: white.instagram.com [157.240.198.63,2a03:2880:f244:ca:face:b00c:0:43fe]
Found: ww.instagram.com [157.240.198.174,2a03:2880:f244:1e8:face:b00c:0:4420]
instagram.com
support-instagram.com
l.instagram.com
platform.instagram.com
ww.instagram.com
instagram.clor.instagram.com
z-p42-instagram.clor.instagram.com
a.ms.instagram.com
b.ms.instagram.com
c.ms.instagram.com
d.ms.instagram.com
i.instagram.com
latest.instagram.com
maps.instagram.com
trunkstable.instagram.com
intern.instagram.com
secure.latest.instagram.com
cdinstagram.com
*.instagram.com
graph.instagram.com
prod.instagram.com
a.instagram.com
beta.instagram.com
upload.instagram.com
secure.instagram.com
autodiscover.instagram.com
graphql.instagram.com
copyright--instagram.com
```

The image shows a terminal window with a dark background. At the top, there is a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. Below the menu bar, the terminal displays a list of domain names, each followed by '.com'. The domains are: cdn.instagram.com, *.instagram.com, graph.instagram.com, prod.instagram.com, e.instagram.com, beta.instagram.com, upload.instagram.com, secure.instagram.com, autodiscover.instagram.com, graphql.instagram.com, copyright.instagram.com, www.copyright.instagram.com, channel.security.instagram.com, gcalendars.security.instagram.com, contacts.security.instagram.com, mail.security.instagram.com, security.instagram.com, webdisk.security.instagram.com, webmail.security.instagram.com, www.security.instagram.com, mail.instagram.com, channel.mail.instagram.com, mail.mail.instagram.com, webdisk.mail.instagram.com, webmail.mail.instagram.com, www.mail.instagram.com, unknownjapan.instagram.com, engineering.instagram.com, www.engineering.instagram.com, partners.business.instagram.com, api.instagram.com, badges.instagram.com, blog.instagram.com, business.instagram.com, demo.instagram.com, distilleryimage0.ak.instagram.com, distilleryimage1.ak.instagram.com, distilleryimage1.ak.instagram.com, distilleryimage18.ak.instagram.com, distilleryimage19.ak.instagram.com, distilleryimage11.ak.instagram.com, distilleryimage2.ak.instagram.com, distilleryimage2.instagram.com, distilleryimage3.ak.instagram.com, distilleryimage3.instagram.com, distilleryimage4.ak.instagram.com, distilleryimage4.instagram.com, distilleryimage5.ak.instagram.com, distilleryimage5.instagram.com, distilleryimage6.ak.instagram.com, distilleryimage6.instagram.com, distilleryimage7.ak.instagram.com, distilleryimage7.instagram.com, f-pa2.graph.instagram.com, f-pa2-1.instagram.com, edge-chat.instagram.com, mail.instagram.com, ny-ed-5.instagram.com, ny-ed-2.instagram.com, ny-ed-4.instagram.com, ny-ed-1.instagram.com, web.instagram.com, web.instagram.com, privacycenter.instagram.com, pmdmccf0e.latest.instagram.com, en-gb.latest.instagram.com, help.hyperlane.beta.latest.instagram.com, f-pa2-1.instagram.com, www.intern.instagram.com, developer.instagram.com, f-pa2.upload.instagram.com, safety.instagram.com, beta.latest.instagram.com, developers.latest.instagram.com, survey.instagram.com, f-pa2-graph.instagram.com, f-pa2-0y1.www.instagram.com, black.instagram.com, f-pa2.maps.instagram.com, instagram-www.instagram.com, graphfallback.instagram.com, fallback.cdn.instagram.com, creators.instagram.com, www.instagram.com, webared390e.11.v111.instagram.com, www-bdsb5bya.instagram.com, i.secure.instagram.com, familycenter.instagram.com, i.b.instagram.com, alltests.instagram.com, white.isb.instagram.com, black.isb.instagram.com, isb.instagram.com, p.instagram.com, cdn.instagram.com, www.help.instagram.com, dountomre.instagram.com, 93873ad6b1d.instagram.com, www1.instagram.com, e23f9e5dc9f.instagram.com, instagram.cdn.facebook.comwww.instagram.com, star-mini.cdn.facebook.comwww.instagram.com, chat.instagram.com, 2fbusines.instagram.com, busnes.instagram.com, iran-geo-pa2.instagram.com, 2fwww.instagram.com, 2fhelp.instagram.com, 2fnewsrcinstagram.com, https://instagram.cdn.instagram.com, https://x-pa2-istagram.cdn.instagram.com, http://instagram.cdn.instagram.com, https://instagram.com, https://l.instagram.com, http://instagram.com, https://platform.instagram.com, https://www.instagram.com, http://www.instagram.com, https://1.instagram.com, https://support.instagram.com, http://1.instagram.com, https://tuntable.instagram.com, https://6.instagram.com, http://x.instagram.com, https://graph.instagram.com, https://ad.instagram.com, https://atnre.instagram.com, https://graph.instagram.com, http://prod.instagram.com, http://intern.instagram.com, http://platform.instagram.com, https://upload.instagram.com, http://upload.instagram.com, https://secure.instagram.com, https://graphql.instagram.com, https://secure.latest.instagram.com, http://secure.instagram.com, https://graphql.instagram.com, http://secure.latest.instagram.com, https://support.instagram.com, http://1.instagram.com, https://maps.instagram.com, http://maps.instagram.com, https://unknownjapan.instagram.com, https://unknownjapan.instagram.com, https://badges.instagram.com, https://badges.instagram.com, https://blog.instagram.com, https://blog.instagram.com, https://autodiscover.instagram.com, https://api.instagram.com, https://api.instagram.com, https://business.instagram.com, https://business.instagram.com, https://engineering.instagram.com, https://engineering.instagram.com, https://gateway.instagram.com, https://geo.instagram.com, https://geo-pa2.instagram.com, https://white.instagram.com, https://b.secure.instagram.com.

```
Running Aquatone
aquatone v1.7.0 started at 2023-09-12T01:45:49-04:00

Targets : 157
Threads : 2
Ports : 80, 81, 443, 591, 2882, 2087, 2095, 2096, 3000, 8000, 8001, 8008, 8080, 8083, 8443, 8534, 8588
Output dir : .

https://platform.instagram.com: 200 OK
https://instagram.c10r.instagram.com: 400 default_vip_400
https://instagram.com: request timeout
https://z-p4-1.instagram.c10r.instagram.com: request timeout
https://instagram.com: request timeout
https://instagram.c10r.instagram.com: request timeout
https://i.instagram.com: request timeout
https://accountscenter.instagram.com: request timeout
https://www.instagram.com: 200 OK
https://www.instagram.com: 200 OK
https://i.instagram.com: 200 OK
https://www.instagram.com: request timeout
https://i.instagram.com: 200 OK
https://www.instagram.com: request timeout
https://www.instagram.com: request timeout
https://w.instagram.com: 200 OK
https://graph.instagram.com: request timeout
https://w.instagram.com: request timeout
https://prod.instagram.com: 404 Not Found
https://graph.instagram.com: 400 Bad Request
https://intern.instagram.com: 400 Bad Request
https://prod.instagram.com: request timeout
https://intern.instagram.com: request timeout
https://platform.instagram.com: request timeout
https://upload.instagram.com: request timeout
https://upload.instagram.com: 200 OK
https://secure.instagram.com: 200 OK
https://secure.instagram.com: request timeout
https://secure.latest.instagram.com: 200 OK
https://secure.instagram.com: 200 OK
https://graphql.instagram.com: 500 Internal Server Error
https://secure.latest.instagram.com: request timeout
https://l.instagram.com: 200 OK
https://maps.instagram.com: 404 Not Found
https://support.instagram.com: 200 OK
https://unknownjapan.instagram.com: 403 Forbidden
https://www.instagram.com: request timeout
https://unknownjapan.instagram.com: 403 Forbidden
https://badges.instagram.com: 500 Internal Server Error
https://badges.instagram.com: 200 OK
https://blog.instagram.com: 200 OK
https://blog.instagram.com: 200 OK
https://autodiscover.instagram.com: 200 OK
https://api.instagram.com: 500 Internal Server Error
https://api.instagram.com: 200 OK
https://business.instagram.com: 200 OK
https://admin.instagram.com: request timeout
https://z-p4-graph.instagram.com: 400 Bad Request
https://pagesapi.instagram.com: request timeout
https://about.instagram.com: 200 OK
https://logger.instagram.com: 404 Not Found
https://z-p4-graph.instagram.com: 400 Bad Request
https://about.instagram.com: 200 OK
https://dyi.www.instagram.com: 403 Forbidden
https://z-p15.www.instagram.com: 200 OK
https://z-p15.www.instagram.com: 200 OK
https://h.l.instagram.com: 200 OK
https://logger.instagram.com: 404 Not Found
https://dyi.www.instagram.com: 403 Forbidden
https://h.l.instagram.com: request timeout
https://en-gb.latest.instagram.com: 200 OK
https://accountscenter.instagram.com: 200 OK
https://wellbeing.instagram.com: 200 OK
https://preprod.instagram.com: 200 OK
https://aplink.instagram.com: 200 OK
https://upload-ec2.instagram.com: 200 OK
https://community.instagram.com: 200 OK
https://z-p3.www.instagram.com: 200 OK
https://help.latest.instagram.com: 200 OK
https://wellbeing.instagram.com: request timeout
https://upload-ec2.instagram.com: 200 OK
https://community.instagram.com: 200 OK
https://www.secure.instagram.com: 200 OK
https://help.latest.instagram.com: 200 OK
https://www.secure.instagram.com: request timeout
https://z-p3.www.instagram.com: request timeout
https://z-p42.www.instagram.com: 200 OK
https://z-p42.www.instagram.com: 200 OK
https://lookaside.instagram.com: 403 Forbidden
https://lookaside.instagram.com: 403 Forbidden
https://z-p4.www.instagram.com: 200 OK
https://z-p42-graph.instagram.com: 400 Bad Request
https://devtools.instagram.com: request timeout
https://z-p4-l.instagram.com: request timeout
https://z-p42-graph.instagram.com: 400 Bad Request
https://edge-chat.instagram.com: 404 Not Found
```

```
root@kali: /home/kali/Documents

File Actions Edit View Help

http://apiprod.instagram.com: request timed out
https://instagram.c10r.instagram.com: screenshot successful
https://www.instagram.com: screenshot successful
https://platform.instagram.com: screenshot successful
http://www.instagram.com: screenshot successful
https://i.instagram.com: screenshot successful
https://l.instagram.com: screenshot successful
https://n.instagram.com: screenshot successful
https://prod.instagram.com: screenshot successful
http://graph.instagram.com: screenshot successful
https://intern.instagram.com: screenshot successful
https://secure.instagram.com: screenshot successful
http://upload.instagram.com: screenshot successful
http://secure.instagram.com: screenshot successful
https://secure.latest.instagram.com: screenshot successful
https://graphql.instagram.com: screenshot successful
http://l.instagram.com: screenshot successful
https://maps.instagram.com: screenshot successful
http://support.instagram.com: screenshot successful
https://unknownjapan.instagram.com: screenshot successful
http://unknownjapan.instagram.com: screenshot successful
https://badges.instagram.com: screenshot successful
http://badges.instagram.com: screenshot successful
https://blog.instagram.com: screenshot successful
http://blog.instagram.com: screenshot successful
https://api.instagram.com: screenshot successful
https://api.instagram.com: screenshot successful
http://autodiscover.instagram.com: screenshot successful
https://business.instagram.com: screenshot successful
http://engineering.instagram.com: screenshot successful
http://business.instagram.com: screenshot timed out
https://geo.instagram.com: screenshot successful
https://white.instagram.com: screenshot successful
https://z-secure.instagram.com: screenshot successful
https://geo-p42.instagram.com: screenshot successful
https://z-p42.l.instagram.com: screenshot successful
https://engineering.instagram.com: screenshot successful
http://geo.instagram.com: screenshot successful
https://help.instagram.com: screenshot successful
https://admin.instagram.com: screenshot successful
http://parents.instagram.com: screenshot successful
https://shortwave.instagram.com: screenshot successful
https://hyperlapse.instagram.com: screenshot successful
http://shortwave.instagram.com: screenshot successful
http://help.instagram.com: screenshot successful
https://z-p4-graph.instagram.com: screenshot successful
https://logger.instagram.com: screenshot successful
http://z-p4-graph.instagram.com: screenshot successful
https://about.instagram.com: screenshot successful
https://about.instagram.com: screenshot successful
https://eyi.www.instagram.com: screenshot successful
https://eyi.www.instagram.com: screenshot timed out
http://eyi.www.instagram.com: screenshot timed out
https://h.l.instagram.com: screenshot timed out
http://logger.instagram.com: screenshot successful

https://upload-ec2.instagram.com: screenshot successful
https://help.latest.instagram.com: screenshot successful
http://community.instagram.com: screenshot successful
https://www.secure.instagram.com: screenshot successful
http://z-p42.www.instagram.com: screenshot successful
https://z-p4.www.instagram.com: screenshot successful
https://lookaside.instagram.com: screenshot successful
http://help.latest.instagram.com: screenshot successful
http://lookaside.instagram.com: screenshot successful
https://z-p42.graph.instagram.com: screenshot successful
http://z-p4.www.instagram.com: screenshot successful
https://z-p42.graph.instagram.com: screenshot successful
https://edge-chat.instagram.com: screenshot successful
https://edge-chat.instagram.com: screenshot successful
https://privacycenter.instagram.com: screenshot successful
https://ew-gb.latest.instagram.com: screenshot successful
https://safety.instagram.com: screenshot successful
https://www.intern.instagram.com: screenshot successful
https://help.hyperlapse.beta.latest.instagram.com: screenshot successful
https://z-p42.eyi.www.instagram.com: screenshot successful
https://z-p15.graph.instagram.com: screenshot successful
http://www.intern.instagram.com: screenshot successful
http://z-p42.eyi.www.instagram.com: screenshot successful
https://z-p42.maps.instagram.com: screenshot successful
https://star.fallback.c10r.instagram.com: screenshot successful
http://star.fallback.c10r.instagram.com: screenshot successful
https://graph-fallback.instagram.com: screenshot successful

Calculating page structures ... done
Clustering similar pages ... done
Generating HTML report ... done

Writing session file ... Time:
- Started at : 2023-09-12T01:45:10-04:00
- Finished at : 2023-09-12T01:56:13-04:00
- Duration : 10m24s

Requests:
- Successful : 91
- Failed : 66

- 2xx : 52
- 3xx : 0
- 4xx : 35
- 5xx : 4

Screenshots:
- Successful : 83
- Failed : 8

Wrote HTML report to: aquatone_report.html
```

Figure 6.1: Script Output Screenshots(Subdomaains)

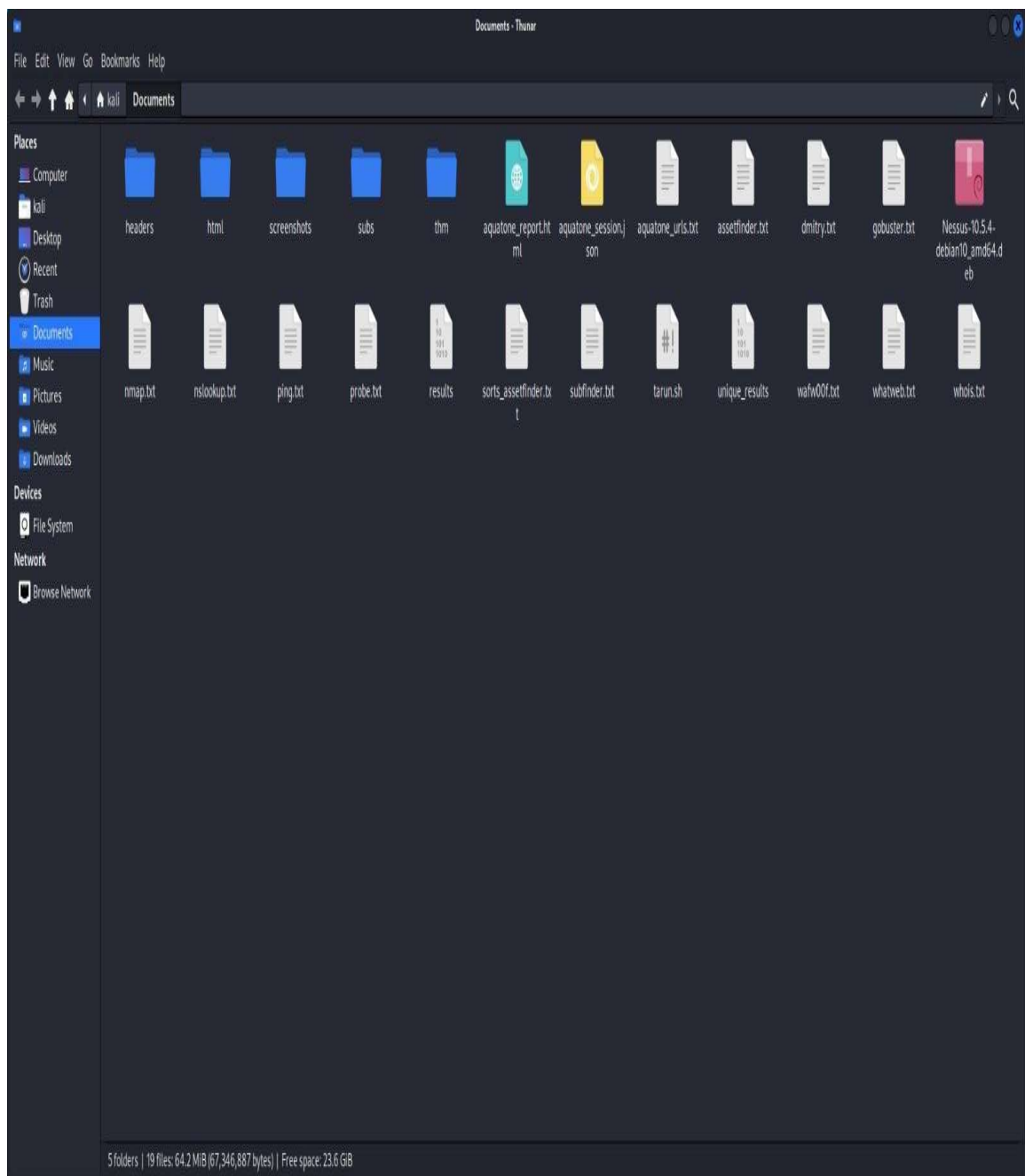


Figure 6.2: Script Generated Files

```
File Edit Search View Document Help
1 https://instagram.c10r.instagram.com
2 https://z-p42-instagram.c10r.instagram.com
3 http://instagram.c10r.instagram.com
4 https://instagram.com
5 https://i.instagram.com
6 http://instagram.com
7 https://platform.instagram.com
8 https://www.instagram.com
9 http://www.instagram.com
10 https://i.instagram.com
11 https://support-instagram.com
12 http://i.instagram.com
13 https://trunkstable.instagram.com
14 http://trunkstable.instagram.com
15 https://n.instagram.com
16 http://n.instagram.com
17 https://graph.instagram.com
18 https://prod.instagram.com
19 https://intern.instagram.com
20 https://graphql.instagram.com
21 http://prod.instagram.com
22 http://intern.instagram.com
23 http://platform.instagram.com
24 https://upload.instagram.com
25 http://upload.instagram.com
26 https://secure.instagram.com
27 https://graphql.instagram.com
28 https://secure.latest.instagram.com
29 http://secure.instagram.com
30 http://graphql.instagram.com
31 http://secure.latest.instagram.com
32 http://support-instagram.com
33 http://i.instagram.com
34 https://maps.instagram.com
35 http://maps.instagram.com
36 https://unknownjapan.instagram.com
37 http://unknownjapan.instagram.com
38 https://badges.instagram.com
39 http://badges.instagram.com
40 https://blog.instagram.com
41 https://blog.instagram.com
42 http://antidiscovers.instagram.com
43 https://api.instagram.com
44 http://api.instagram.com
45 https://business.instagram.com
46 http://business.instagram.com
47 https://engineering.instagram.com
48 http://engineering.instagram.com

21 https://geo-pvz.instagram.com
52 https://white.instagram.com
53 https://b.secure.instagram.com
54 https://parents.instagram.com
55 https://z-p42.i.instagram.com
56 http://geo-p42.instagram.com
57 https://geo.instagram.com
58 https://help.instagram.com
59 https://admin.instagram.com
60 http://parents.instagram.com
61 https://shortwave.instagram.com
62 http://white.instagram.com
63 https://b.secure.instagram.com
64 https://hyperlapse.instagram.com
65 http://z-p42.i.instagram.com
66 http://admin.instagram.com
67 http://help.instagram.com
68 http://shortwave.instagram.com
69 http://hyperlapse.instagram.com
70 https://z-p4-graph.instagram.com
71 http://z-p4-graph.instagram.com
72 https://about.instagram.com
73 https://logger.instagram.com
74 http://about.instagram.com
75 https://z-p45.www.instagram.com
76 https://dyi.www.instagram.com
77 https://z-p45.www.instagram.com
78 https://b.i.instagram.com
79 http://logger.instagram.com
80 http://dyi.www.instagram.com
81 http://b.i.instagram.com
82 https://accountscenter.instagram.com
83 http://accountscenter.instagram.com
84 https://wellbeing.instagram.com
85 https://preprod.instagram.com
86 https://applink.instagram.com
87 https://upload-ec2.instagram.com
88 https://community.instagram.com
89 http://wellbeing.instagram.com
90 https://z-p3.www.instagram.com
91 https://help.latest.instagram.com
92 https://applink.instagram.com
93 http://upload-ec2.instagram.com
94 https://community.instagram.com
95 https://www.secure.instagram.com
96 https://help.latest.instagram.com
97 http://www.secure.instagram.com
98 https://z-p42.www.instagram.com
```

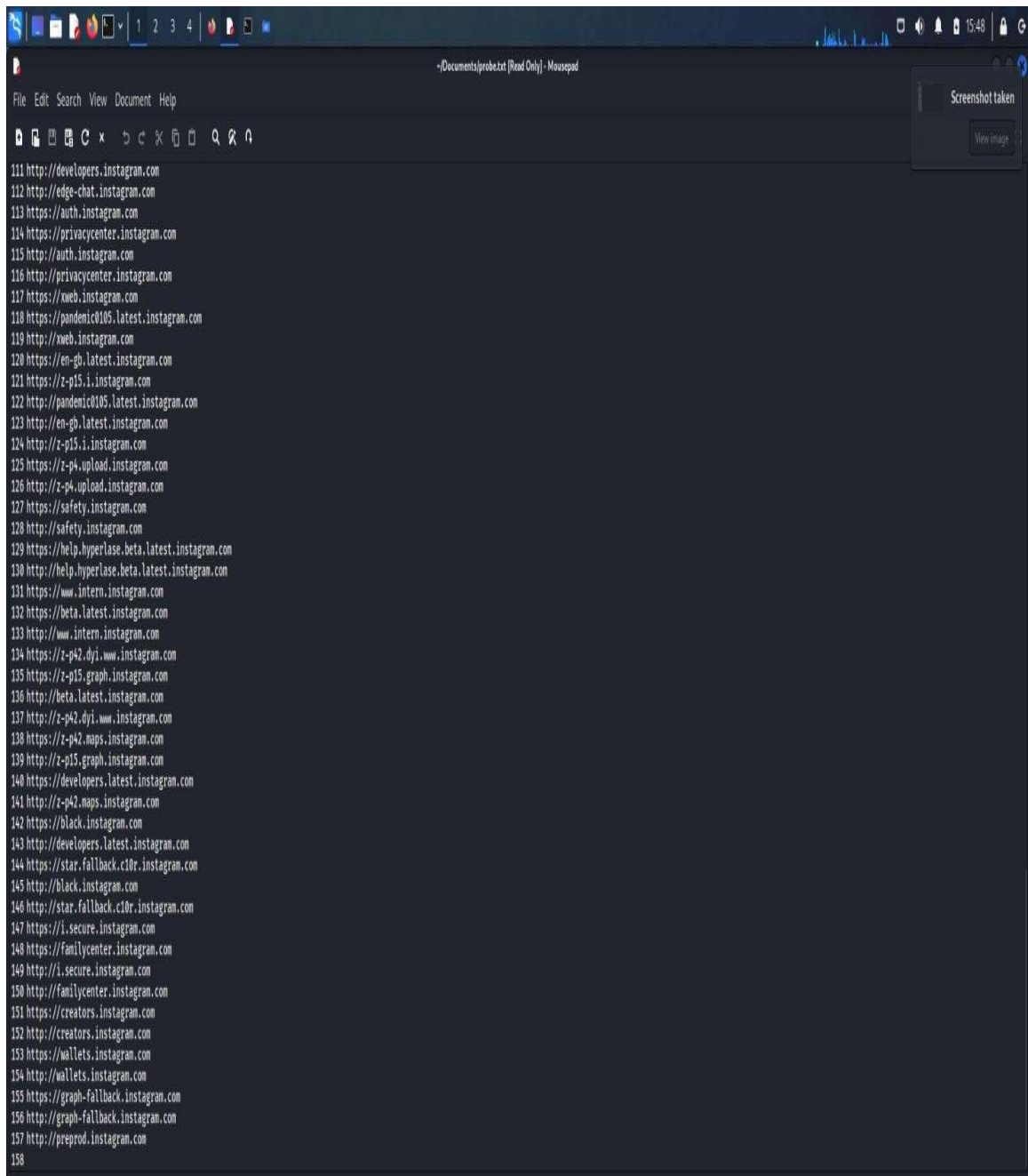



Figure 6.3: Probe.txt (Contains all the valid subdomains)

7. Conclusion

In the dynamic and evolving landscape of cybersecurity, where threats loom around every virtual corner, the importance of comprehensive threat assessment cannot be overstated. Subdomains, often overlooked but critical components of a domain's attack surface, require dedicated attention to identify vulnerabilities and mitigate risks effectively. The script presented in this report addresses this need by automating the subdomain enumeration process, providing accuracy, saving valuable time, and ensuring data integrity.

Subdomain enumeration, a fundamental step in cybersecurity assessments, was traditionally a manual and time-consuming endeavor, fraught with challenges. Manual enumeration was prone to errors, inaccuracies, and oversights, hindering the efficiency and efficacy of threat assessments. Moreover, in the rapidly evolving cybersecurity landscape, delays in identifying subdomains could lead to severe consequences.

The script, powered by a synergy of well-established subdomain enumeration tools such as Dmitry, Anew, Gobuster, Assetfinder, Httpprobe, Subfinder, and Aquatone, rises to these challenges with a multifaceted approach. It streamlines the enumeration process, ensuring data accuracy, automating tedious tasks, and significantly reducing the time required for comprehensive assessments. Herein lies its significance.

Through automation, the script alleviates the burden of manual enumeration, offering the ability to process vast volumes of subdomains with precision. By merging the outputs of various tools and eliminating duplicates using Anew, it creates a consolidated list of unique subdomains, ensuring data integrity and accuracy. The combination of Gobuster, Assetfinder, Subfinder and Httpprobe allows it to efficiently identify subdomains, validate their accessibility, and determine their operational status.

In conclusion, the script's automation and efficiency significantly contribute to the early detection of threats and vulnerabilities, providing cybersecurity professionals with a powerful tool to bolster their assessments. By mitigating the challenges associated with subdomain enumeration, it empowers practitioners to stay ahead in the ever-escalating battle against cyber threats. Its role in enhancing cybersecurity cannot be understated, making it an invaluable asset for professionals dedicated to safeguarding digital landscapes. As the cyber threat landscape continues to evolve, tools like this script become essential allies in the ongoing mission to protect digital assets and ensure a secure digital future.

8. References

- Linux Command Line and Shell Scripting Bible 4th Edition
- Mastering Linux Shell Scripting: A practical guide to Linux command-line, Bash scripting, and Shell Programming, 2nd Edition
- blog.appsecco.com
- www.educba.com
- OWASP (Open Web Application Security Project): <https://owasp.org/>
- Dmitry GitHub Repository: <https://github.com/jaygreig86/dmitry.git>
- Gobuster GitHub Repository: <https://github.com/OJ/gobuster>
- Assetfinder GitHub Repository: <https://github.com/tomnomnom/assetfinder>
- Subfinder GitHub Repository: <https://github.com/projectdiscovery/subfinder.git>
- Anew GitHub Repository: <https://github.com/tomnomnom/anew.git>
- Bash Scripting Guide : <http://tldp.org/LDP/abs/html/index.html>

