International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

AUTOMATED RECONNAISSANCE TOOL FOR PENTESTING ENGAGEMENTS

***Sundeep Varma* [*1], *Jonnadula Narasimharao*[*2]**

*[*1]Student, Computer science and engineering, CMR Technical campus, Medchal, Telangana, India*
*[*2]Associate Professor, Computer science and engineering, CMR Technical campus, Medchal, Telangana, India*

ABSTRACT

Reconnaissance, more generally called recon, denotes the information gathered before planning the real attacks. This is done in the initial stage of any attack. The effectiveness of an attack solely depends on the recon done, as a result making this phase an important part of the process. Careful analysis is needed to be done which takes up a good amount of time. The information collected is of different types and from different sources. Most important in any cyber assessment is the technical information, This includes IP-ranges, Sub domains, web technologies, insight of networks and infrastructures, hardware being used and sometimes as crucial as passwords. There are few tools to achieve a particular task in the process of reconnaissance. This paper explores a tool which harvests the Strong suit of the open source tools and subjoins them to perform an effective and smooth reconnaissance. It offers 2 modes of ctf and bug bounty. This tool can be added to the arsenal of any ctf player or bug hunter to perform an efficient Reco

***Keywords**: Port scanning, Reconnaissance, sub domain enumeration, web attacks, bug bounty, CTF*

1. INTRODCUTION

Security engagements like pentesting or hacking in general consists of 5 phases namely Reconnaissance,Scanning, Gaining access,Maintaining access and covering tracks.[8] The entire cycle of hacking starts with reconnaissance. The motive of this phase is to gather information about the target and get familiar with the target system and network. Reconnaissance itself is done in different sections i.e. footprinting, scanning and enumeration ultimately to reveal information about the target system.

Active reconnaissance is a technique in which the information gathered about the target is through an active engagement with the target. This is done through automated scanners, pining the system and manual testing. As the active engagement is made with the system it is easy to detect and is risky. But the results obtained are faster and accurate. Port Scanning is one of the important active reconnaissance techniques. Which is done using a famous tool called NMAP which is used in the project.[9]

Passive reconnaissance is a technique where we don't engage with the target system but the information can be gathered through different resources such as googling the target, OSINT for ip addresses,emails,host names,DNS records, checking cms and associated CVEs..

Once information like open ports are obtained, services running on the ports are checked, based on the service running and version number they are further investigated to find any CVE or any exploit for the obtained service and version.In most of the cases there is a web server running which should be enumerated again attacks like directory brute forcing. This brute forcing is done to obtain hidden subdomains. Once the subdomains are obtained then web attacks must be done on those to check for the vulnerabilities. Attacks like xss,sqli,LFI,File upload etc[5] are done. In case of bug bounty subdomains have to be enumerated from different sources. As different sources and tools are used the duplicates are generated. These duplicates should be removed and check if all the hosts are running and live.

As explored, reconnaissance is a vast task with lots of techniques and tools. There are good tools on the internet which achieve a specific task of reconnaissance. If there's a ctf the user has to use all the tools one after another to perform reconnaissance. As there are many tools employed, the user has to remember the syntax of all the tools with flags which can be hard to remember.Even if the syntax is remembered, the user has to run one tool after another. Repeat the same process on the next engagement. There are few automated tools but mostly are paid. This projects explores all the tools best for the specific task and chains them together to form a tool where if only the ip is given the port scanning, service enumeration, exploit suggestion, directory brute forcing and web attacks are automatically performed

2. BACKGROUND

2.1 Port Scanning

Port scanning is a technique to know which ports are open on a system and actively listening. This is done by sending data packets to specific or all ports of the target and investigating the response to determine the possible vulnerabilities. This can reveal the security measures in place such as a firewall. Different types of port scanning is done. Ping scans, Syn scans, Xmas scans etc. Each scan is different from others but they serve the same purpose.[1]

2.2 Subdomains

Subdomains are an additional part of primary domains. They are created to organize the sections of the web page, They operate under the same domain name. Subdomains allow us to create new websites under the same domain. A best example of this is few websites use location specific websites such as in.site.com or uk.site.com . [2][3]

2.3 Web Attacks

As websites have become an important part of marketing. They have been developed with different features like subscribing articles, submitting a query, submitting a form etc. All this data must be stored, processed and transferred and these tasks are done by employing web applications which help manage different functions. This makes web applications a risk factor as different attacks are performed on them. The motive behind these attacks can be as simple as deforming the structure of a web page or something serious as gaining sensitive information or access to the databases.

Different types of web attacks are performed like XSS, SQL injection, Local file inclusion, IDORs, File uploads are etc. Owasp has a good list of web attacks. As web applications are risky they must be checked for all possible web attacks before it goes on the internet.[4][5]

2.4 CTFS

Capture the flag events more generally called ctfs are security competitions where players are given few cyber security challenges and the to solve. This can be as basic as programming exercise and as complex as hacking your way into the server to steal a specific piece of data which is called flag and hence its called Capture the flag. Big organizations like Google run their ctf events. These are large cash rewards. Different types of challenges given ranging from cryptography, Web,pwn,OSINT etc.[6]

2.5 Bug Bounty

Bug bounties are bug hunting programs where security researchers and hackers ethically hack the company websites to detect the bugs and report the vulnerabilities directly to the company if there are any. These hackers are rewarded for discovering vulnerabilities.Companies leverage the skills of the hacker community to improve the security of their systems.[7]

3. METHODOLOGY

As mostly the bug bounty players or cyber security enthusiasts in general prefer command line tools over a gui version the tool is designed as a command line utility. Acknowledgements

3.1 Project Architecture

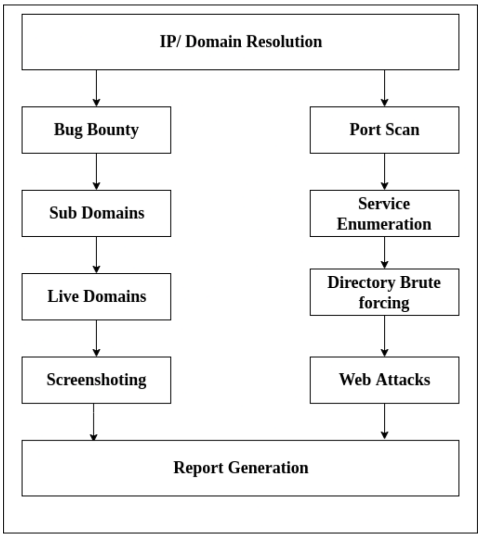


Figure 1: Architecture of the reconnaissance tool.

- **IP Module: ip** modules the ip is taken and analyzed for missing values or domain lookup is done.
- **Port Scan**: Nmap is made Scan on the target for checking the open ports. Common exploits are made search on the obtained running services[9]
- **Sub domains** : Sub domains are analyzed and obtained with various tools Live Subdomains Active and live subdomains are filtered by HTTPX[14]
- **Screenshot ting** : Screenshot ting is done using eyewitness or aquatone
- **Directory brute forcing** : Directory brute forcing is done using gobuster or dirbuster with common seclist wordlist
- **Web Attacks** :Web Attacks like sql injection ,xss , rce, injection attacks are performed using various tool

3.2 Activity Diagram

The input is given by the user, depending upon the module selected i.e. either a ctf module or a bug bounty module the flow changes. If the ctf module is chosen then the given ip is checked if it's valid. If it's valid then the first step is initiated i.e. port scanning. using Nmap[9] an aggressive post scan is done with -T4 which gets all the live ports and services running. Using awk only the ports and services are obtained. Port 80 or 443 is checked. If the target has the http(s) ports open then directory brute forcing is done using gobuster[10] with medium dirb wordlist. Searchsploit is run on obtained ports and services to enumerate possible exploits. At last using uniscan[11] different web attacks are performed that includes xss, SQLI, File upload etc.

If the user chooses the Bug bounty module then the input domain is checked for the validity with some regex validity is confirmed. If the input domain seems to be valid then sublister[12] is run to obtain subdomains. This tool searches through google,bing,DNS dumpster, virus total,SSL certificates and different sources to obtain subdomains. Second round of subdomain enumeration is done with the assetfinder[13] which crawls through crt.sh, certspotter, threatcrowd,wayback machine to obtain the assets and subdomains. The third round of subdomain enumeration is done with subfinder to enumerate more domains. When done all these subdomains are checked for the duplicates which are removed and unique domains are obtained. These unique domains are then passed through httprobe[14] to check if they are live. When the live domains are obtained aquatone is employed to gather screenshots. In the end a python module called FPDF is used to create a pdf report of findings.

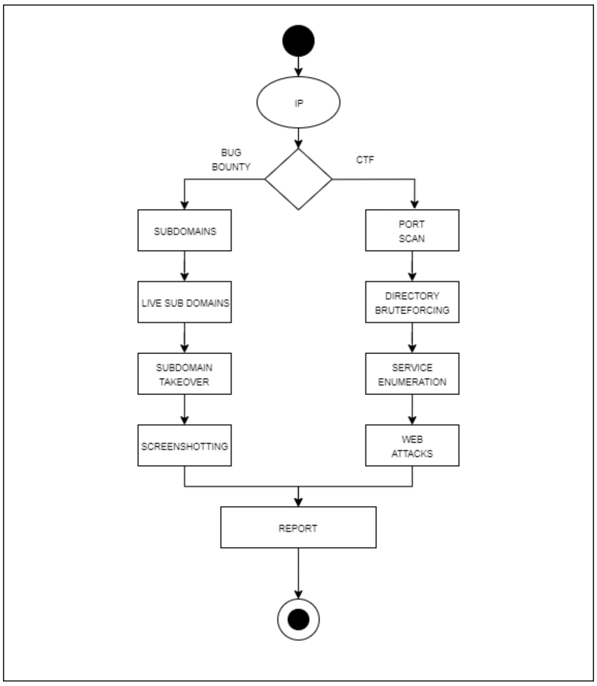


Figure 2: Activity diagram of the reconnaissance tool.

3.3 Sequence Diagram

The bug bounty module is chosen. The domain is entered by the user as input domain. This domain is checked and valid domain is obtained, with the valid domain subdomain enumeration is done. After sub domain enumeration is done all the domains are obtained. These domains are then checked for the live status. After all the live domains are obtained, subdomain takeover is checked. In the end a PDF report is generated. This report is presented to the user.

If the user enters the target ip as command line argument, the tool takes the input ip and checks if it's valid . The valid ip is passed to the ctf module where port scanning is done and all the active ports are obtained and passed to service enumeration. In service enumeration the services running on the ports are obtained along with version numbers. This is further passed to search for exploits. Directory brute forcing is done on the given ip. Web attacks are performed and results of the entire process are presented to the user.

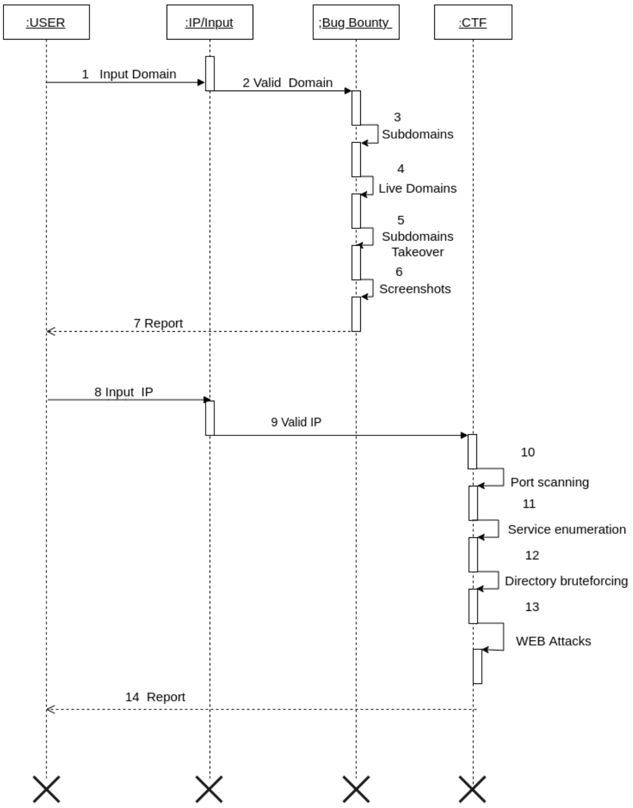
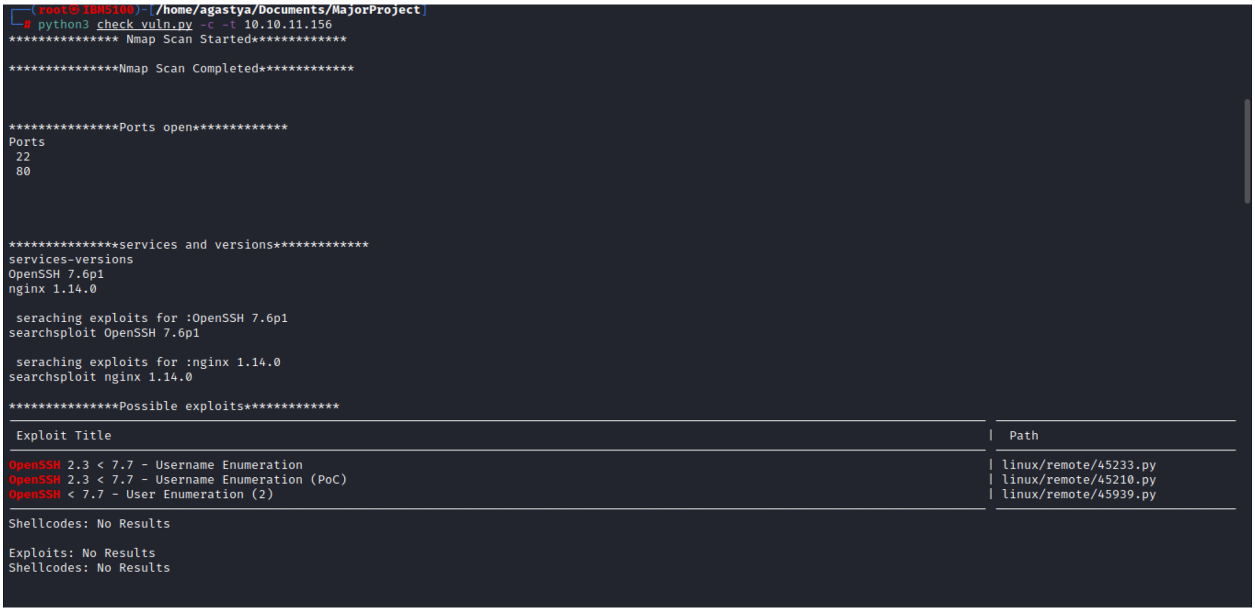


Figure 3: Sequence diagram of the reconnaissance tool.

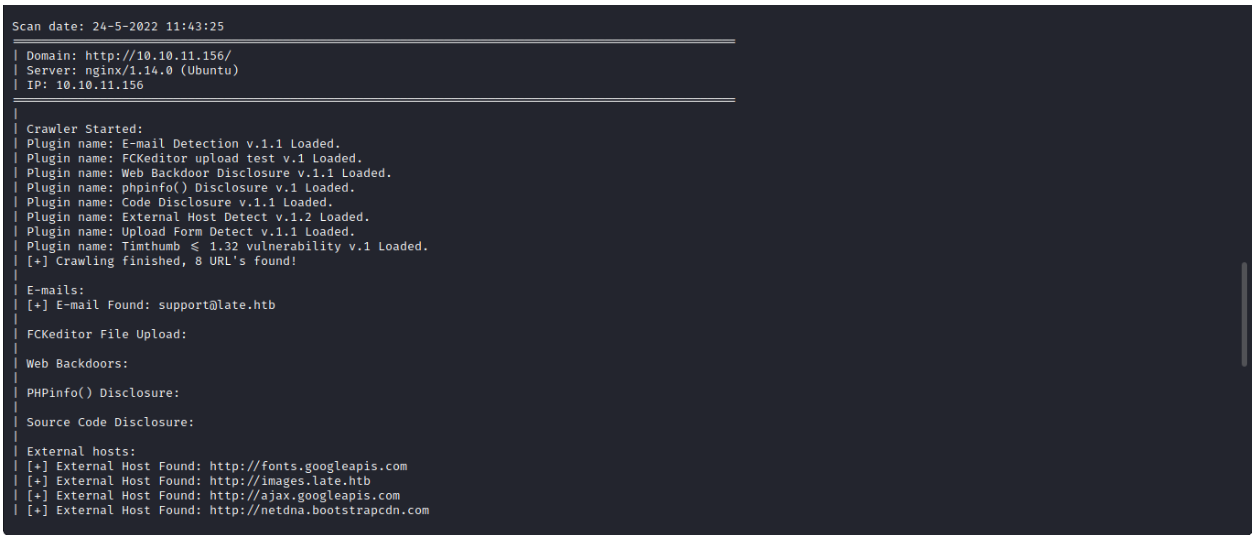
4. RESULTS AN DISCUSSION

To test out the the tool I have signed up to hack the box and a tool on a machine and the results for the ctf modules are obtained



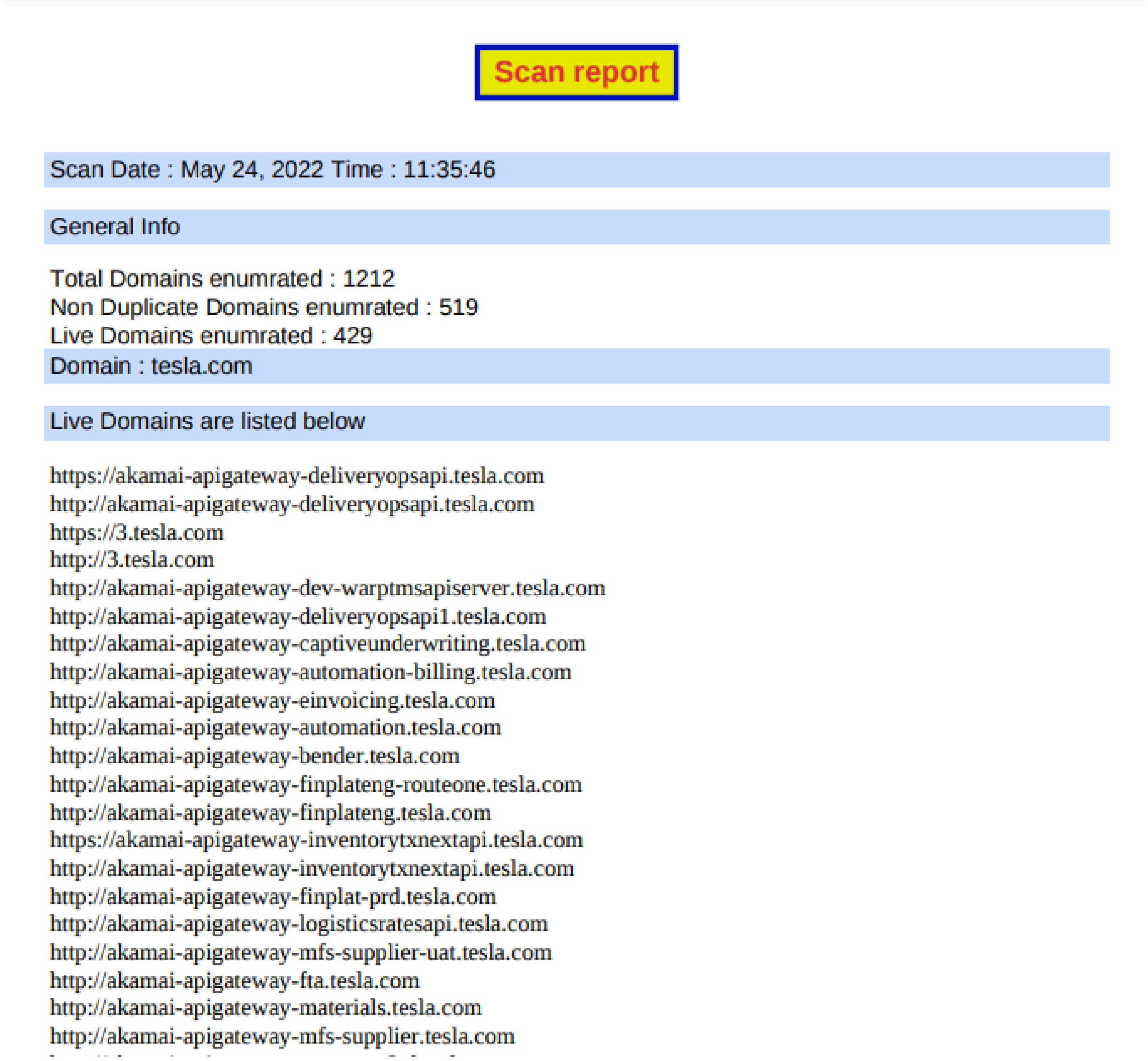
```
┌──(root㉿IBM5100)-[/home/agastya/Documents/MajorProject]
└─# python3 check_vuln.py -c -t 10.10.11.156
*************** Nmap Scan Started*************

***************Nmap Scan Completed*************



***************Ports open*************
Ports
 22
 80



***************services and versions*************
services-versions
OpenSSH 7.6p1
nginx 1.14.0

 seraching exploits for :OpenSSH 7.6p1
searchsploit OpenSSH 7.6p1

 seraching exploits for :nginx 1.14.0
searchsploit nginx 1.14.0

***************Possible exploits*************
 ------------------------------------------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                                                  |  Path
 ------------------------------------------------------------------------------------------------------------------------------- ---------------------------------
OpenSSH 2.3 < 7.7 - Username Enumeration                                                                                       | linux/remote/45233.py
OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)                                                                                 | linux/remote/45210.py
OpenSSH < 7.7 - User Enumeration (2)                                                                                           | linux/remote/45939.py
 ------------------------------------------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results

Exploits: No Results
Shellcodes: No Results
```

Figure 4: Ports can and service scan



```
Scan date: 24-5-2022 11:43:25
═══════════════════════════════════════════════════════════════════════════════════════════════════
| Domain: http://10.10.11.156/
| Server: nginx/1.14.0 (Ubuntu)
| IP: 10.10.11.156
═══════════════════════════════════════════════════════════════════════════════════════════════════
|
| Crawler Started:
| Plugin name: E-mail Detection v.1.1 Loaded.
| Plugin name: FCKeditor upload test v.1 Loaded.
| Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
| Plugin name: phpinfo() Disclosure v.1 Loaded.
| Plugin name: Code Disclosure v.1.1 Loaded.
| Plugin name: External Host Detect v.1.2 Loaded.
| Plugin name: Upload Form Detect v.1.1 Loaded.
| Plugin name: Timthumb ≤ 1.32 vulnerability v.1 Loaded.
| [+] Crawling finished, 8 URL's found!
|
| E-mails:
| [+] E-mail Found: support@late.htb
|
| FCKeditor File Upload:
|
| Web Backdoors:
|
| PHPinfo() Disclosure:
|
| Source Code Disclosure:
|
| External hosts:
| [+] External Host Found: http://fonts.googleapis.com
| [+] External Host Found: http://images.late.htb
| [+] External Host Found: http://ajax.googleapis.com
| [+] External Host Found: http://netdna.bootstrapcdn.com
```

Figure 5: web attacks



Scan report

Scan Date : May 24, 2022 Time : 11:35:46

General Info

Total Domains enumrated : 1212
Non Duplicate Domains enumrated : 519
Live Domains enumrated : 429

Domain : tesla.com

Live Domains are listed below

https://akamai-apigateway-deliveryopsapi.tesla.com
http://akamai-apigateway-deliveryopsapi.tesla.com
https://3.tesla.com
http://3.tesla.com
http://akamai-apigateway-dev-warptmsapiserver.tesla.com
http://akamai-apigateway-deliveryopsapi1.tesla.com
http://akamai-apigateway-captiveunderwriting.tesla.com
http://akamai-apigateway-automation-billing.tesla.com
http://akamai-apigateway-einvoicing.tesla.com
http://akamai-apigateway-automation.tesla.com
http://akamai-apigateway-bender.tesla.com
http://akamai-apigateway-finplateng-routeone.tesla.com
http://akamai-apigateway-finplateng.tesla.com
https://akamai-apigateway-inventorytxnextapi.tesla.com
http://akamai-apigateway-inventorytxnextapi.tesla.com
http://akamai-apigateway-finplat-prd.tesla.com
http://akamai-apigateway-logisticsratesapi.tesla.com
http://akamai-apigateway-mfs-supplier-uat.tesla.com
http://akamai-apigateway-fta.tesla.com
http://akamai-apigateway-materials.tesla.com
http://akamai-apigateway-mfs-supplier.tesla.com

Figure 6: subdomain enumeration

5. CONCLUSION

In this paper we have explored what reconsaance is and types of it and how important it is for any security engagements. As reconnaissance is an important test and needs manual effort to run tools and enumerate. Using this tool during any pentesting engagements or CTFs and bug bounties in general this will automate the entire process and generates a pdf report using this report pentesters can focus on what's important and save enough time

6. ACKNOWLEDGMENT

We thank CMR Technical Campus for supporting this paper titled with " ***Automated Reconnaissance Tool For Pentesting Engagements***" which provided good facilities and support to accomplish our work. Sincerely thank to our Chairman, Director, Deans,Head Of the Department, Department Of Computer Science and Engineering, Guide and Teaching and Non- Teaching faculty members for giving valuable suggestions and guidance in every aspect of our work.

REFERENCES

[1] Avast, 'What is port scanning' , accessed 1,july,2022, https://www.avast.com/business/resources/what-is-port-scanning#pc

[2] wpbeginner. 'What is subdomain' , accessed 1,july,2022, https://www.wpbeginner.com/glossary/subdomain/

[3] Kevin Wood, 19,oct,2022 , 'what is a subdomain', accessed 1,july,2022, https://www.hostgator.com/blog/whats-a-subdomain/

[4] TrustNet, 'Common Web Application Attacks', accessed 1,july,2022, https://www.trustnetinc.com/web-application-attacks/

[5] OWASP, 'OWASP Top Ten', accessed 1,july,2022, https://owasp.org/www-project-top-ten/

[6] Atan, 28,Mar,2019, 'What is CTF and how to get started!', accessed 1,july,2022, https://dev.to/atan/what-is-ctf-and-how-to-get-started-3f04

[7] Computerfutures, 'All you need to know about bug bounty hunting', accessed 1,july,2022, https://www.computerfutures.com/en-jp/blog/2020/12/all-you-need-to-know-about-bug-bounty-hunting/

[8] Sudip Sengupta, 22,Oct, 2021, 'What are the 5 steps of ethical hacking' , accessed 1,july,2022, https://crashtest-security.com/five-steps-of-ethical-hacking/

[9] Nmap, 'Nmap', accessed 1,july,2022, https://nmap.org/

[10] DRD, 8,july,2019, 'Scan Websites for Interesting Directories & Files with Gobuster', accessed 1,july,2022, https://null-byte.wonderhowto.com/how-to/scan-websites-for-interesting-directories-files-with-gobuster-0197226/

[11] DRD, 16,Feb,2019, 'Detect Vulnerabilities in a Web Application with Uniscan', accessed 1,july,2022, https://null-byte.wonderhowto.com/how-to/detect-vulnerabilities-web-application-with-uniscan-0193207/

[12] HACKING TUTORIALS, 14, Nov,2017, 'Discovering subdomains with Sublist3r', accessed 1,july,2022 ,https://www.hackingtutorials.org/web-application-hacking/discovering-subdomains-with-sublist3r/

[13] gaurav gandal, 28 Jul, 2021, 'Assetfinder – Find domains and subdomains related to a given domain' , accessed 1,july,2022 , https://www.geeksforgeeks.org/assetfinder-find-domains-and-subdomains-related-to-a-given-domain/

[14] Rickard, 21, Jan, 2020, 'HTTPROBE', 'accessed 1,july,2022 ', https://tzusec.com/httprobe/