CREATING BUG BOUNTY AUTOMATION FRAMEWORK USING BASH

(Major-Project Phase 1 review)

A project report submitted to the Srinivas University as partial fulfilment for the award of the degree of

Bachelor of Technology in Cloud Technology and Information Security

Submitted By

ANAND C

USN: 1SU19CI006

Under the Guidance of

Dr A. SASI KUMAR

Professor

Department of Cloud Technology & Data Science
Institute of Engineering and Technology
SRINIVAS UNIVERSITY
Mukka, Mangalore – 574146

BONAFIDE CERTIFICATE

This is to certify that this project report entitled "**Creating Bug Bounty Automation Framework using Bash**" is submitted to Srinivas University College of Engineering and Technology, Mukka, is a bonafide record of work done by **ANAND C**

Dr A. Sasi Kumar
Professor

Prof. Daniel Selvaraj
Head of Department
Department of Cloud Technology and Data Science
Srinivas University, Mukka

Date:

Place: Mukka

TABLE OF CONTENTS

ABSTRACT

Bug bounty can directly be associated with reconnaissance. The need for Recon automation is rapidly increasing as ethical hackers are being lazy in performing every little check manually. To make the Recon process (Info gathering phase) of penetration testing or bug bountying easy, and accurate, a Recon framework with highly sophisticated tools written in languages like bash, go and python needs to be developed and made open source to everyone. Manually doing this task can be very intimidating since a lot of time and efforts are needed in accomplishing this task.

Automation of this task can be very handy to the penetration testers and saves a lot of time as they can focus on other tasks of the further tasks of a penetration test. So, our project is an automation to the tedious task of information gathering. This Recon Framework just takes the main top-level domain of the organization as the input, does the recon and stores the result in an organized manner in the corresponding directories.

Keywords— Recon, penetration testing, Automation

INTRODUCTION

CYBER SECURITY

The explosive growth of the web has brought many goodies like E-commerce, E-mail, Cloud computing, but there's also a black side of Hacking, malwares etc. Hacking is one of the biggest problems faced by tech companies, governments, and citizens across the world. An Ethical Hacker or a Penetration tester can assist or help the people that are suffering from these cyber-attacks. Ethical hacking is usually termed as online geeks or groups that legally access the company's online assets after obtaining official approval. Reconnaissance means the preparatory stage where an Ethical Hacker seeks to collect the maximum amount of information as possible a few targets before launching a security test. It involves 3 phases namely, scanning, foot printing, and enumeration of the organization's network.

In this project, we'll be handling automation of foot printing of an organization. Foot printing is nothing but the blueprint of the safety of a corporation, undergone during a procedural manner. It finds all information available on the internet about the target. It is a time-taking process to flick through the sites and collect info; hence in this paper, we investigate the solution for tedious web search and propose a proficient way to organize, extract and store data from the search engines employing a new tool, Search Simplified.

Reconnaissance is key to any successful hacks. On average, approximately three-fourths of any hack should be spent performing accurate and precise reconnaissance. Reconnaissance is the act of gaining information about our targets. Such as all subdomain, active subdomain, open ports, operating systems, what services those ports are running, screenshot of UI and any vulnerable applications they have installed. All of this information will be absolutely important to choosing an attack

There are two base types of recons, active and passive. Both have their pros and cons, so let's cover these types of recons briefly:

Active: This includes intrusive recon that sends (specially built) data to the target, for example, port-scanning. Advanced network foot printing techniques dodge direct connections with the target host.

Passive: This is the kind of reconnaissance that either does not contact or communicate directly to the target system or that uses publicly available information, and not normally found from standard logs. This paper also focuses on this technique.

Both active and passive reconnaissance can cause the invention of useful data to use in a malicious activity. This information may enable an attacker to seek out vulnerabilities in the OS's version and exploit the loophole to gain more access. Shell-script based Recon Framework is a fully featured recon framework which is written in shell script. It provides a great environment where open-source reconnaissance is often carried out in a timely and thorough manner.

Tools and services which are generally used

WHOIS

Whois is a protocol that fetches WHOIS record against a domain name form the domain registrar. WHOIS record includes many crucial information like:

- Registrar: Via which registrar was the domain name registered
- Detail of registrant: Name, organization, address, phone, email & etc (these info can be made hidden by activating paid privacy services)
- Creation, update and expiration dates of the domain
- Name Server: Which DNS server is used for name resolution

NSLOOKUP

Nslookup stands for Name Server Lookup used for querying the Domain Name System to fetch DNS records against a domain.

DIG

Dig stands for Domain Information Groper, it also fetches DNS record form DomainName server (does the same thing like nslookup) but is one of hackers favourite tool because it returns more information as compared to other tools. Syntax is dig -trecord_type DOMAIN_NAME @SERVER

DNSDUMPSTER

DNS Dumpster is a domain research online tool and its speciality is that it also provides hidden subdomain (host information) along with other DNS record information (like DNS servers, MX records, TXT records & Host records) against a domain in a well organized manner. It also tries to resolve domain names to IP addresses and even tries to get their geo location.

To use just go to 'https://dnsdumpster.com/' and enter target domain in the search query & just a single search will be enough to fetch all the mentioned information.

IOT SEARCH ENGINE

There are IOT search engines like shodan, censys and natlas that help us search forvarious types of systems connected to the internet and services running on them based on different filters. They can be used for a variety of things like mapping and gathering information about internet-connected devices or can even be used to learn various pieces of information about a targeted client's network without even being the part of the network.

These types of search engines can provide a lot of information about any internet connected device; some of them are IP address, hosting company, geographical location, server type, ports opened, services running, versions and more.

FULLHUNT

Full Hunt is also an online tool that claims to be the attack surface database of the entire Internet. It searches for all the internet facing assets against a provided domain and scans for open services, ports and technologies. It also tries to figure out possible attack surfaces and vulnerabilities for the organization

GITHUB GREP

Grep. app is an online search engine for GitHub repositories, it will present a list of repositories that matches our search query. It can be important for finding hidden/open information from source code and discovering sensitive information like api, db creds, ftp creds, and much more

SUBLIST3R

Sublist3r is a python based tool which helps to find subdomains of a website using Open-Source Intelligence. It gathers information from open resources like search engines (Google, Bing, Yahoo), Netcraft, Virus Total, DNS Dumpster, Threat Crowdand Reverse DNS

CERTIFICATE SEARCH — CRT

Crt.sh is online website which has certificate transparency logs of every registered domain. It can be used to find subdomains, as it provides details of every domain and subdomain including certificate issuer name. To use it we only need to enter a domain in the search query

EMAIL SEARCH

Hunter.io and phonebook.cz can be used to find various email addresses related to a company's domain

WAPPALYZER

Wappalyzer is a browser extension that gives instant information about a website's technology like CMS, CDN, framework, ecommerce platform, JavaScript libraries, programming languages used and more just by visiting the website

WAYBACK MACHINE

Wayback Machine is a digital archive of the World Wide Web, it allows us to go ‘back in time’ and see how websites looked in the past. Which can be a great help for us to figure out the technologies being used by seeing the previous version and also tobfind some mistakes in the website which has been removed in recent update. To use it just go to ‘https://archive.org/web/’ and search the target’s URL

Both active and passive reconnaissance can cause the invention of useful data to use in a malicious activity. This information may enable an attacker to seek out vulnerabilities in the OS’s version and exploit the loophole to gain more access. Shell-script based Recon Framework is a fully featured recon framework which is written in shell script. It provides a great environment where open-source reconnaissance is often carried out in a timely and thorough manner.

1.1 THE DOMAIN

Cyber security could be defined as the procedure to ease the security fears in order to protect repute damage, commercial loss or financial loss of all group. The term Cybersecurity obviously required that it’s a gentle of security that we proposal to the organisation that frequent users can contact using the internet or over a network. There are numerous tackles and techniques that are castoff to deploy it. The greatest significant fact around safeguarding information is that it’s not a one interval procedure but a non-stop process. The organisation proprietor has to keep stuffs modernised in mandate to keep the hazard low.

The definitive objective of cybersecurity is to defend the data from actuality stolen or co-operated. To attain this, we aspect at the three important goals of cybersecurity.

1. Defensive the Privacy of Information
2. Conserving the Integrity of Information
3. Controlling the Obtainability of information only to approved users

These objectives practise the confidentiality, integrity, availability (CIA) triad, the base of entirely safety agendas. This CIA triad mode is a safety model that is intended to guide strategies for data security inside the places of a society or corporation. This model is similarly mentioned to in place of the AIC (Availability, Integrity, and Confidentiality) triad to side-step the mistake with the Central Intelligence Agency. The rudiments of the triad are reflected the three greatest vital mechanisms of safety.

The CIA standards are one that greatest of the societies and businesses practice once they have connected a new request, makes a record or when assuring access to approximately information. On behalf of data to be totally safe, all of these safe keeping areas must originate into result. These are safe keeping strategies that all effort together, and hence it can be incorrect to supervise one policy. CIA triad is the greatest collective standard to measure, choice and appliance the proper safety panels to condense risk.

Confidentiality

Making guaranteed that your complex statistics is reachable to accredited users and safeguarding no information is revealed to unintended ones. In case, your key is private and will not be shared who power adventure it which ultimately hampers Confidentiality.

Integrity

Make sure all your data is precise; dependable and it must not be changed in the show from one fact to another.

Availability

Every time the operator has demanded a resource for a portion of statistics there shall not be any bout notices like as Denial of Service (DoS). Entirely the evidence has to be obtainable.

1.2 THE PROBLEM STATEMENT

The bug bounty industry has experienced a significant growth in the past few years. Now, more and more companies are running their bug bounty program and accepting reports from hackers around the world. Worldwide competition, along with a rapidly growing number of programs requires hackers to be either very creative in finding unique bugs or to automate part of their workflow, as only the first hacker reporting a bug gets paid.

Numerous hackers have proven that the financial gain from a large-scale bug bounty automation may be in hundreds of thousands of dollars per year.

Most of those tools are kept private, and there are only very few attempts to release a unified, open-source automation framework, similar to Metasploit in the penetration testing field. Bug bounty, being a very young and competitive scene, lacks a common platform for automation of tedious tasks. Various open-source command line tools are released frequently, but there is currently no common framework that would allow combining them easily. Even if such a framework is created, it is either kept private or shared only in small groups with the indisputable motivation of receiving a bounty.

1.3 THE TECHNOLOGY USED

Passive reconnaissance

Reconnaissance is the first and the most important step in Hacking. It is the process of discovering and collecting as much possible information about our target system or organization. After a proper Recon an attacker can plan its further attack strategy against its target including social engineering and technical attacks. Passive reconnaissance includes various activities like looking for DNS records from public DNS servers, checking ads and posts related to the organization, reading news articles related to the target, checking publicly available certificates, visiting social media pages and surfing its website as a normal user.

Bash

Bash is a command processor that typically runs in a text window where the user types of commands that cause actions. Bash can also read and execute commands from a file, called a shell script. Like most Unix shells, it supports filename globing (wildcard matching), piping, here documents, command substitution, variables, and control structures for condition-testing and iteration. The keywords, syntax, dynamically scoped variables and other basic features of the language are all copied from sh. Other features, e.g., history, are copied from csh and ksh. Bash is a POSIX-compliant shell, but with a number of extensions. The shell's name is an acronym for Bourne Again Shell, a pun on the name of the Bourne shell that it replaces and the notion of being "born again”. Bash is a legitimate interface to your computer, and it's not just for server admins and programmers.

TOOLS

Finding Subdomains:

subbrute

SubDomainizer

subfinder

Sublist3r

Amass

assetfinder

knock

Discovering endpoints:

Hakrawler

gobuster

ffuf

LinkFinder

dirsearch

Scanning:

SecretFinder

Ports & Services:

Nmap

masscan

naabu

Vulnerability scanning:

nuclei

Sn1per

D-TECT-1

xray

Useful Websites:

DNSdumpster : discover hosts related to a domain

WHOIS : whois information, DNS, domain names, name servers, IPs,…

ICANN: look up the current registration data for domain names and Internet number resources

Crunchbase : Discover innovative companies and the people behind them

BuiltWith : Technology lookup

Domain Dossier : Free online network tools

DNSlytics : online investigation tool

SpyOnWeb : SEO research tool that helps optimize your website for search engines

Virus Total : analyzes suspicious files, URLs, domains and IP addresses to detect malware and other types of threats

Visual Ping : Website change detection and alert

View DNS : check all DNS records of a domain.

Pentest-Tools : online penetration testing tools

Spyse : identify internet assets and perform external reconnaissance

crt.sh : find all the SSL or TLS certificates

Shodan : search for various types of servers (webcams, routers, servers, etc.) connected to the internet

Wayback Machine : digital archive of the World Wide Web

Open Corporates : shares data on corporations

AI HIT : unique source of company information

Netcraft

Security Headers

SSL Server Test

Pastebin

Extensions:

Wappalyzer, WaybackMachine, whatruns

1.4 EXISTING SYSTEMS

The existing models available today have very limited features and are not compatible with the modern web development frameworks like MEAN and MERN stacks, Django, Flask or Spring Framework. As these new technologies and tech stacks came into limelight, there are many things which are overlooked and often many vulnerabilities are missed when tried with the existing recon frameworks. Some of the important things missed by the existing recon frameworks are:

- JavaScript file enumeration and analysis.
- Automation of Google Dorking
- Automation of some known OWASP vulnerabilities like XSS, SSRF etc.
- Absence of project discovery’s nuclei at the time of writing old recon frameworks.
- Automation of fuzzing for endpoints on the target.

Since the existing frameworks did not incorporate multi-threading in their tools, the recon process takes a lot of time. The output management hasn't been up to the mark in any of the frameworks. And in addition to that, each recon framework lacks one or the other features like speed, accuracy, etc. These are the limitations of the existing models and thus there is a need for a fast and accurate framework which automates every single module of the information gathering phase.

SYSTEM ANALYSIS

2.1 LITERATURE REVIEW

Nagendran K et.al in [1] explains the technical approach to perform a manual penetration test in web applications for testing the security of the applications and it serves as a great guide to look for security vulnerabilities. It provides us with various techniques to secure web apps from hackers. Ahana Roy et.al in [2] says that they proposed a tool which gathers the footprint of a corporation, helpful for information gathering phase during a penetration test and it is found that there is a lack of an easy tool which can help in the first stage of such penetration tests; Reconnaissance. The Java-based tool greatly helps in gathering organization-specific data. These data storages help greatly in vulnerability evaluation of a firm. Kristian Beckers et.al in [3] describes the details of a survey done on tools in 2017 which are there for social engineering and intelligence gathering. It presents an outline of their specifications and capabilities. It describes that attacker have a wide range of Opensource intelligence gathering tools which greatly increases the likelihood of the attacks in the future.

Usman Ali Dar et.al in [4] explores different kinds of reconnaissance techniques that are used by an attacker or hacker to collect information regarding the target. It determines which technique gathers the most info about the target while keeping itself hidden to the internet. Dr Arun Kumar et.al in [5] explains that as Web Apps are increasingly used for complex services, they become a popular and great target for security attacks. Plenty of techniques have been developed to secure web applications and stop the attacks towards web apps, there is a very little effort devoted to drawing conclusions among these techniques and developing a broader view of the web application security research. This paper gives an outlined examination of assaults against picked critical parameters.

S.M. Zia Ur Rashid et.al in [6] describes that the Domain name system has been an essential part of cyber security and an essential part of the web services used. The nameservers are completely responsible for the safety and functionality of their domain names. But as there is lag of ample security and DNS misconfiguration, there can be a chance to take over the subdomain from the external services. This paper mainly focuses on detailed analysis on subdomain takeover, map out the bug's impact on the firm. Tae Hyun Kim et.al in [7] describes that DNS is used to provide scalable name resolution services to the users in an easy and efficient manner. However, DNS was developed without security initially, and the data is not secured. We describe the overview of DNS bugs, DNS attacks, and even protection systems. In detail, attacks are divided by purpose and techniques for defending against the attacks that are introduced and analysed. The important findings of this work is to introduce basic vulnerabilities of DNS. The paper [8] describes that is easy to find logs and bugs in server-side applications but when we use client-side applications it is more complex. The front end of client-side applications uses Angular, React etc which flags the way for vulnerabilities. The static analysis is performed to find vulnerabilities like secret keys to API, finding domains, Potential wild card entries etc. Script Hunter by Robre is used for finding JavaScript files. But before using this, we need to install Go properly. The paper [10] tells us that most of the companies are using frameworks like React, Vue, Ember etc instead of JavaScript. However, there are various tools to convert them to JavaScript. Dev Tools tab is used to inspect JavaScript code in Chrome. Map files give us a way to go through the original source code. Arjun Guha et.al in [11] describes that in static analysis, we need to identify and gather JavaScript files, make the JavaScript file readable and finding security issues. Jaspher Kathrine et.al in [12] tells us about the patterns which play a vital role in Subdomain Enumeration. Since, the patterns like qa, dev, staging, api, uat are repeatedly used by the developers in naming the subdomains, enumeration of subdomains can be done easily by brute forcing these patterns. Rizdqi Akbar Ramadan et.al in [13] explains the importance of performing ample reconnaissance that will increase the chance of finding vulnerabilities. Subdomain Enumeration techniques are also explained here. Mayur Parmar in [14] uses search string which uses advanced options to find the hidden information. It is useful for bug bounties for performing network mapping, port scanning, information gathering etc.

Marco Squarcina et.al in [15] defines the threats posed by related-domain attackers to web application security. The paper describes on some vulnerabilities like CORS(Cross-Origin Resource Sharing), CSP(Content-Security Policy) bypass, postMessage and domain relaxation. Suraj S. Mundalik et.al in [16] explores information gathering techniques and the attack simulation implementation that is done particularly with Kali Linux OS by using various pentesting tools. Kali Linux OS makes it easier to perform pen testing on the target host with the help of its huge tool set which is free of cost and present in open source. He also emphasises on a basic overview of the various tools present in the Kali Linux Operating System. Sushmitha

Reddy Mamilla in [17] explains her project that compares some basic scanning tools in terms of the no. of ports found open and the time taken by the tool to find those open ports. A cmprehensive analysis of the results generated by the tools will be used to find the efficient tools.

Monowar et.al in [18] tells us about port scans performed by attackers to discover weak systems to compromise. This paper also discusses about the common port scanning attacks. Marco de Vivo et.al in [19] describes the techniques that the TCP port scanners use. Administrators also use port scanning to prevent the unwanted exploitation by the port scanners. It also describes the various services' vulnerabilities that can be found on those pen ports. Vinitha K in [20] explains the basic security issues in the modern web applications and also describes the types of hackers. This paper also focuses on the various ethical hacking phases which are being used by both hackers and penetration testers too. Bowman Miller in [21] focuses on the importance of OSINT by telling the fact of having special wings for OSINT in US Air Force, US Dept of State and many other government organizations of the nation. This paper also describes the various OSINT techniques used in World War II. Javier Pasto-Galindo et.al in [22] describes the Opportunities, open challenges and Future Trends of the OSINT techniques and methodologies. This paper emphasises on the fact that a ton of information available to gather information about everything.

2.2 HARDWARE AND SOFTWARE REQUIREMENTS

HARDWARE REQUIREMENTS

- Recommended to run on Vpcs with 1VCPU
- Minimum 2GB RAM
- Minimum 50 GB Storage

OPERATING SYSTEM

- Linux based Operating System (Kali Linux or Parrot OS preffered)

SOFTWARE REQUIREMENTS

- Python
- Go

2.3 PROPOSED SYSTEM

Keeping in view the existing models, this proposed model is an attempt to overcome the limitations of the existing models and having updated tools and techniques which are mostly based on fingerprints of various endpoints of the target web application.

TABLE I. KEY FEATURES OF PROPOSED MODEL

Sl. No	**Features of the project**
1.	The speed of the recon process is great as the tools are written in Go and Python and support multi-threading.
2.	Nuclei is another great tool in finding low hanging vulnerabilities.
3.	JavaScript enumeration is made simple than ever before.
4.	Dorking is now just one click away as all the main dorks for a target are incorporated in the project.
5.	With evolved wordlists, content enumeration is very effective with our project.

Workflow of the proposed model

- Take the input (top-level domain) from the user as a command line argument to the recon script.
- Perform subdomain enumeration on the target (top level domain name)
- Extract all the live subdomains which have a web server running on them from the enumerated subdomains list.
- Also gather the status codes and titles of the live subdomains
- Perform google dorking on the subdomains.
- Get all the URLs once present on the target from waybackmachine.

- Perform credential stuffing on the target.
- Perform JavaScript enumeration on all the live subdomains.
- Perform fuzzing to find the hidden functionality and content on the subdomains.
- Perform a simple port scan to have an idea of what ports are open and what services are running on them.
- Perform nuclei scan on the target.
- Look for some simple vulnerabilities like Open Redirects, XSS, SSRF on some parameters obtained from the waybackurls.

SYSTEM DESIGN

Flow Diagram of the Proposed Model

This project is designed to create an automated framework for Bug bounty program or Recon phase of an ethical hacking process. The step-by-step process of the working of the proposed model is explained in the form of a flowchart in the figure 1. The flowchart clearly depicts the working flow of the process of how each module of the model helps in gathering information which can be a greatly useful for further phases of a penetration test. Each major task like subdomain enumeration, dorking, JavaScript analysis, content enumeration etc. are termed as a module in this model and thus each module contributes to the final output of the proposed model.

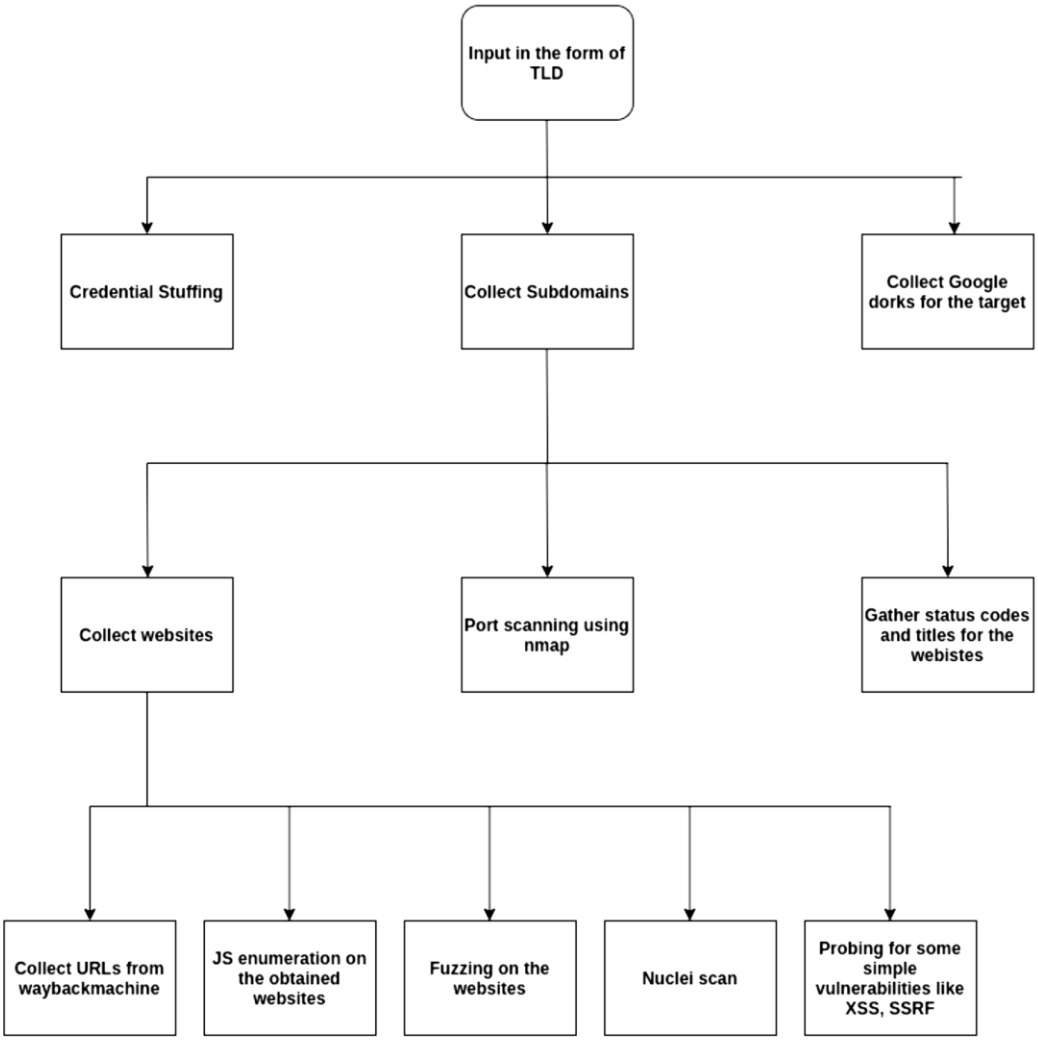
Input in the form of TLD
Credential Stuffing
Collect Subdomains
Collect Google dorks for the target
Collect websites
Port scanning using nmap
Gather status codes and titles for the webistes
Collect URLs from waybackmachine
JS enumeration on the obtained websites
Fuzzing on the websites
Nuclei scan
Probing for some simple vulnerabilities like XSS, SSRF

Fig 1: Flow Diagram of the proposed model

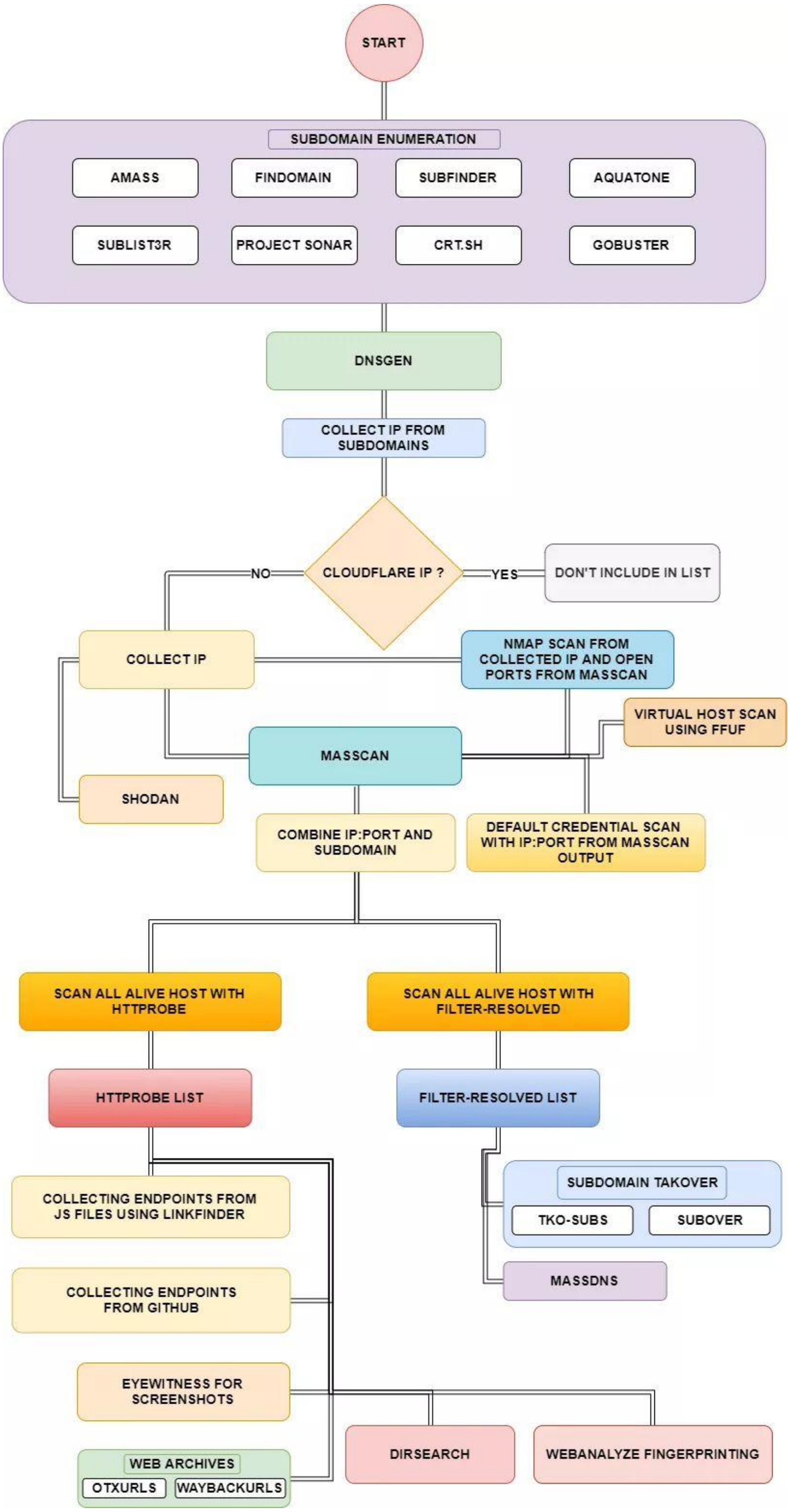
START
SUBDOMAIN ENUMERATION
AMASS
FINDOMAIN
SUBFINDER
AQUATONE
SUBLIST3R
PROJECT SONAR
CRT.SH
GOBUSTER
DNSGEN
COLLECT IP FROM SUBDOMAINS
CLOUDFLARE IP ?
NO
YES
DON'T INCLUDE IN LIST
COLLECT IP
NMAP SCAN FROM COLLECTED IP AND OPEN PORTS FROM MASSCAN
VIRTUAL HOST SCAN USING FFUF
MASSCAN
SHODAN
COMBINE IP:PORT AND SUBDOMAIN
DEFAULT CREDENTIAL SCAN WITH IP:PORT FROM MASSCAN OUTPUT
SCAN ALL ALIVE HOST WITH HTTPROBE
SCAN ALL ALIVE HOST WITH FILTER-RESOLVED
HTTPROBE LIST
FILTER-RESOLVED LIST
COLLECTING ENDPOINTS FROM JS FILES USING LINKFINDER
SUBDOMAIN TAKOVER
TKO-SUBS
SUBOVER
MASSDNS
COLLECTING ENDPOINTS FROM GITHUB
EYEWITNESS FOR SCREENSHOTS
DIRSEARCH
WEBANALYZE FINGERPRINTING
WEB ARCHIVES
OTXURLS
WAYBACKURLS

Fig 2: Functioning of proposed model

CONCLUSION

This project created for easing Recon phase runs scripts that first creates a few empty directories where the results of the script are stored. Then, the subdomain enumeration starts, and all the subdomains are stored in a text file in subdomains folder. Websites (http or https) with their status codes and titles are extracted from the subdomains list, and the credentials from breached data are collected. All the past URLs of the website are collected using waybackurls. Then, JavaScript enumeration starts and collects all the available .js files of the target. Then, project discovery’s nuclei starts its scans and finds some low hanging vulnerabilities. Port scanning does its job by collecting all the open ports, services running on them, and their versions too. Then, hidden content is found using file and directory. Finally, all the results are stored in their respective directories.

The user only needs to do is navigate to the directory of choice and view the text files using any text editor like vim or nano. The penetration tester’s job is greatly reduced to just running the model which is basically a shell script by giving the target’s domain as an argument to the script. The script does its job and shows the results after the execution is completed. Each module’s output is stored in its own directory

REFERENCES

[1] Nagendran K, Adithyan A, Chethana R, Camillus P, Bala Sri Varshini K B "Web Application Penetration Testing," at International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-10, August 2019

[2] Ahana Roy, Louis Mejia, Paul Helling, Aspen Olmsted "Automation of Cyber Reconnaissance: A Java based open-source tool for information gathering", published at 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)

[3] Kristian Beckers, Sebastian Pape, Peter Schaab, Daniel Schosser, "Conference: International Conference on Trust and Privacy in Digital Business", August 2017

[4] Usman Dar, Arsalan Iqbal, "The Silent Art of Reconnaissance: The Other Side of the Hill", January 2018.

[5] Arun Kumar, Sandeep Arora, "A Review on Web Application Security", March 2018

[6] S M Zia Ur Rashid, MD Imtiaz Kamrul, Asraful Islam, "Understanding the Security Threats of Esoteric Subdomain Takeover and Prevention Scheme", published at 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), Feb 2019.

[7] Tae Hyun Kim, Douglas Reeves, "A survey of domain name system vulnerabilities and attacks", January 2020

[8] Andres Ojamaa, Karl Duuna, "Assessing the security of Node.js platform", published at 2012 International Conference for Internet Technology and Secured Transactions, Dec 2012

[9] Nataliia Bielova, "Survey on JavaScript Security Policies and their Enforcement Mechanisms in a Web Browser",published at Journal of Logic and Algebraic Programming, November 2013

[10] Ankur Taly, Ulfar Erlingsson, John C. Mitchell, Mark S. Miller, Jasvir Nagra, "Automated Analysis of Security-Critical JavaScript APIs"

[11] Arjun Guha, Claudiu Saftoui, Shriram Krishnamurthy, "The Essence of JavaScript "

[12] Jaspher Kathrine, Ronnie T Baby, V. Ebenzer, "COMPARATIVE ANALYSIS OF SUBDOMAIN ENUMERATION TOOLS AND STATIC CODE ANALYSIS", ISSN (Online) : 2454 -7190 Vol.-15, No.-6, June (2020) pp 158-173 ISSN (Print) 0973-8975

[13] Rizdqi Akbar Ramada, Redho Maland, Dedi Hariyadi, “Sudomy: Information Gathering Tools for Subdomain Enumeration and Analysis”, The 2nd International Conference on Engineering and Applied Sciences 2019 (2nd InCEAS 2019)At: Yogyakarta, Indonesia, Volume: 771, March 2020

[14] Mayur Parmar, “Google Dorks -Advance Searching Technique”, August 2019

[15] Marco Squarcina, Mauro Tempesta, and Lorenzo Veronese, TU Wien; Stefano Calzavara, “Can I Take Your Subdomain? Exploring Same-Site Attacks in the Modern Web”, Università Ca' Foscari Venezia & OWASP; Matteo Maffei, TU Wien

[16] Suraj S.Mundalik, “Penetration Testing: An Art of Securing the System (Using Kali Linux)”, published at International Journal of Advanced Research in Computer Science and Software Engineering, October 2015

[17] Sushmita Reddy Mamilla, “A Study of Penetration Testing Processes and Tools”, May 2021.

[18] Monawar H. Bhuyan, Dhruba K. Bhattacharya, Jugal Kalita, “Surveying Port Scans and Their Detection Methodologies”, The Computer Journal 54(10):1565-1581, October 2011

[19] Marco de Vivo, Le Ke, Germinal Isern, Gabriela O. de Vivo, “A review of port scanning techniques”, ACM SIGCOMM Computer Communication Review 29(2):41-48, April 1999

[20] Vinitha K P, “Ethical Hacking”, published at INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY, May 2018

[21] Bowman H.Miller, “Open Source Intelligence (OSINT): An Oxymoron?”, December 2018

[22] Javier Paster-Galindo, Pantaleone Nespoli, Felix Gomez Marmol, Gregorio Martinez Perez, “The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends”, January 2020

[23] Himanshu Singh, “Distributed Port Scanning Detection”, 2009

[24] Muharman Lubis, Nurul Ibtisaam Yacoob, Hafizah Binti Reh, Montadzah Ambag Abdulgani, “Study on Implementation and Impact of Google Hacking in Internet Security”, Regional Conference on Knowledge Integration in ICT 2010At: Selangor, June 2011

[25] Mamta Bhavsar, Dr Priyanka Sharma, Manik Gokani, “Port Scanning using Nmap”, published at International Journal of Engineering Development and Research, December 2017.