e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:01/January-2023 Impact Factor- 6.752 www.irjmets.com

TOOL FOR HACKING PHASES

Surya B[*1], Dr. Kumanan T[*2], Dr. Geetha S[*3], Dr. Mehata K M[*4]

[*1]PG Scholar - M.Tech CFIS, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Maduravoyal, Chennai, Tamilnadu, India

[*2]Professor, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Maduravoyal, Chennai, Tamilnadu, India

[*3]Head of Department, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Maduravoyal, Chennai, Tamilnadu, India

[*4]Advisor, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Maduravoyal, Chenna, Tamilnadu, India

ABSTRACT

Ethical hacking is a process of detecting vulnerabilities in an application, system, or organization's infrastructure. This tool is helpful for ethical hackers to perform penetration testing on a system or network. In real life, Ethical Hackers use a lot of tools for penetration testing. Various tools are used for different kinds of purposes. One of the biggest tasks faced by Ethical Hackers is finding tools. This task can be intimidating since a lot of time and effort are needed in accomplishing this task. This tool can be handy to penetration testers and saves a lot of time as they can focus on various tasks of a penetration test. Currently, we have individual tools for phases in hacking to find the vulnerabilities, it takes a lot of time for the user to use a separate tool for each hacking phase. In our project, we have a single tool that includes all five phases of hacking. In the Bug Bounty phase, it has the modules such as Clickjacking, Host Header Injection, and URL Redirection checker. For instance, the first phase is information gathering which has five modules in it. To find the third module, "trace IP' one needs to enter option three and then enter the IP address and the tool traces the IP and gives the information. The same procedure is followed to access different phases and its module accordingly. There are 5 phases in hacking such as reconnaissance, scanning, gaining access, maintaining access, and clear tracking. An attacker or an ethical hacker follows the same five-step hacking process to breach the network or system.

Keywords: Ethical Hacking; penetration testing; Kali Linux; White hat hackers.

I. INTRODUCTION

The main purpose of this project is to facilitate the work of Ethical hackers. Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating the strategies and actions of malicious attackers. An attacker or an ethical hacker follows the same five-step hacking process to breach the network or system. This tool is helpful for ethical hackers to penetration testing on systems or networks. This tool has the tools needed for Ethical hacking phases like reconnaissance, scanning, gaining access, maintaining access, and clear tracking.

II. LITERATURE SURVEY

(Vijaya R Saraswathi et al, 2022) 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 of penetration testing easy, fast, 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. So, 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.

(Aswathy Mohan et al, 2022) Penetration Testing in Ethical Hacking is one of the most efficient methods used by high end organizations to overcome this data threat caused by cyber criminals. Penetration Testing uses a group of Pen testers to perform the cyber-attack done same by unknown hackers but with legal consent from the owners of the organization. They create a generalized report which specifies the set of identified vulnerabilities in the target system in the organization. They also advise countermeasures or solutions to overcome the security weaknesses of the organization.

(Sushmita Reddy Mamilla, 2021) information is more vulnerable than ever, and every technological advance raises new security threat that requires new security solutions. Penetration testing is conducted to evaluate the security of an IT infrastructure by safely exposing its vulnerabilities. It also helps in assessing the efficiency of the defence mechanisms tools and policies in place. The Penetration testing is conducted regularly to identify risks and manage them to achieve higher security standards.

(R. Sri Devi & M. Mohan Kumar, 2020) in the digital world, everything gets connected through the network, and when various services are provided by web applications people are susceptible to hacking. According to the 2019 internet security threat report by Symantec, an average of 4, 800 websites are vulnerable to digital information theft attacks. The main intent of this paper is to recognize openness and flaws in networks and web applications using penetration testing to protect institutions from cyber threats.

(Sudhanshu Raj & Navpreet Kaur Walia, 2020) The usage of internet is everywhere. It plays an important part in the life of humans. As we all know that the Internet has made the life of humans much easier not only in personal but also in professional aspect. This ease in life has given birth to so many threats and flaws that are further giving access to the intruders known as 'Hackers' to enter in a user's private space and perform some activities which can be very harmful for that particular user. In this paper, we will discuss about the Metasploit Framework tool which is always used by the Hackers & Pen-testers to perform activities i.e. from Scanning to exploiting the systems.

1. Existing System

The existing system of this project is only for a particular hacking phase not for all the phases. There was no option for gathering information about websites, finding Instagram information using a username, finding social media accounts using the image, finding multiple social media account with a username, network scanning, port scanning, and mac changer. The existing tool does not give clear details about PDF metadata information, IP address information, Subdomain Information, and Reverse IP information. It doesn't have the tools needed for bug bounty hunting. There was an option for generating payloads for different kinds of a platform like Android, Windows, Linux, iOS, Python, PHP, and Java.

2. Proposing System

The proposed system is a single tool that includes all five phases of hacking which has six modules and twenty-two sub-modules in it. The first module is Information gathering which has the sub-modules such as Instagram Information gathering, Trace IP, PDF metadata analysis, Username enumeration, and social media hunting using the image. The second module is Website vulnerability scanning which has the sub-modules such as Subdomain Enumeration, Reverse IP, and Website Information Gathering. The third module is Network scanning which has the sub-modules such as Network Scanner, Mac changer, and Port scanning. The fourth module is Anatomy of URL which has the sub-modules such as Malicious URL detection and URL shortener. The fifth module is Payload Generator which has the sub-modules such as Android Payload Generator, windows Payload Generator, Apple-iOS Payload Generator, Linux Payload Generator, Python Payload Generator, Java Payload Generator, and PHP Payload Generator. The Bug Bounty module has the sub-modules such as Clickjacking, Host Header Injection, and URL Redirection checker.

3. Architecture Diagram

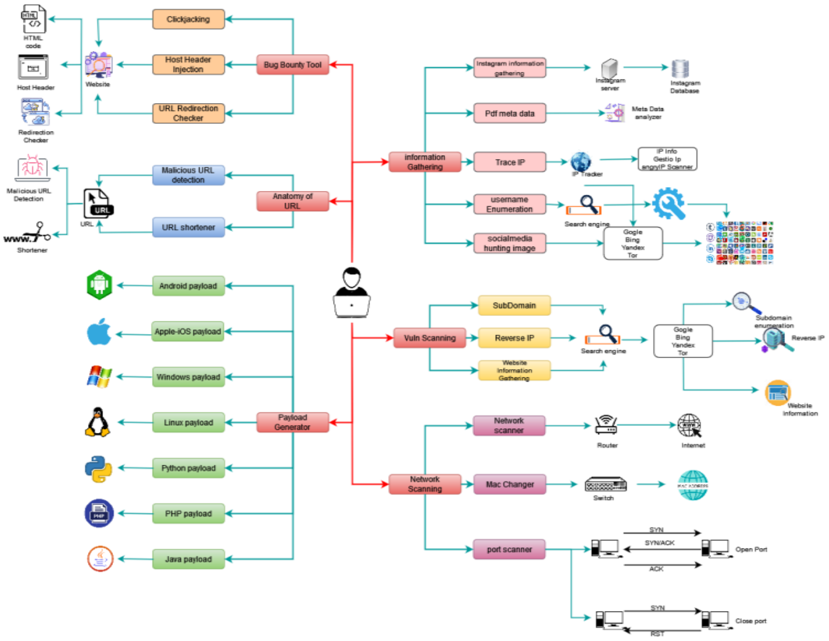


Figure 1. Architecture Diagram

4. List of Phases

There are 6 phases

- Information Gathering
- Website vulnerability scanning
- Network scanning
- Bug Bounty tool
- Anatomy of URL
- Payload Generator

4.1 Information Gathering

This is the first step of Hacking. It is a set of techniques like Foot printing, scanning, and enumeration. The goal of the reconnaissance phase is to identify and gather information about the target.

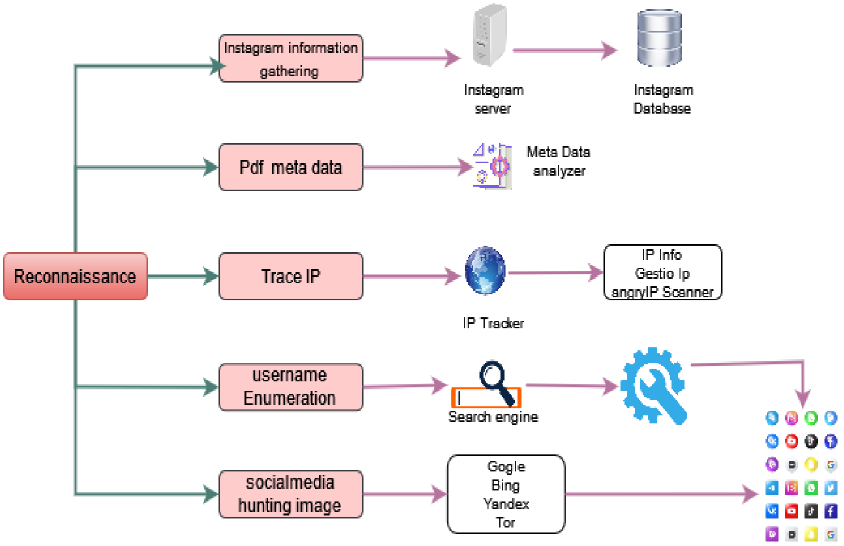


Figure 2. Information Gathering Diagram

The Information Gathering phase of this tool contains options are:

- **Instagram Information Gathering-**The Tool gets a range of information from an Instagram account. The information includes User id, followers/following, number of uploads, profile image URL, business enum, external URL, joined Recently, etc.
- **Trace IP-**Lookup details about an IP address including location, ISP, hostname, type, proxy, and blacklist status.
- **PDF Metadata Analysis-**PDF metadata is data about a PDF document. It provides additional information about a PDF document, including the file name of the document, its title, date of creation, author, copyright information, and what application was used to create the file.
- **Username Enumeration-**Find usernames across over 75 social networks. This is useful if you are running an investigation to determine the usage of the same username on different social networks.
- **Social Media Hunting Using Image-**Hunt down social media accounts by image across social network

4.2 Website Vulnerability Scanning-The second step in the hacking methodology is scanning, and collecting more information using complex and aggressive reconnaissance. Vulnerability scanning is identifying vulnerabilities and weak points in a target.

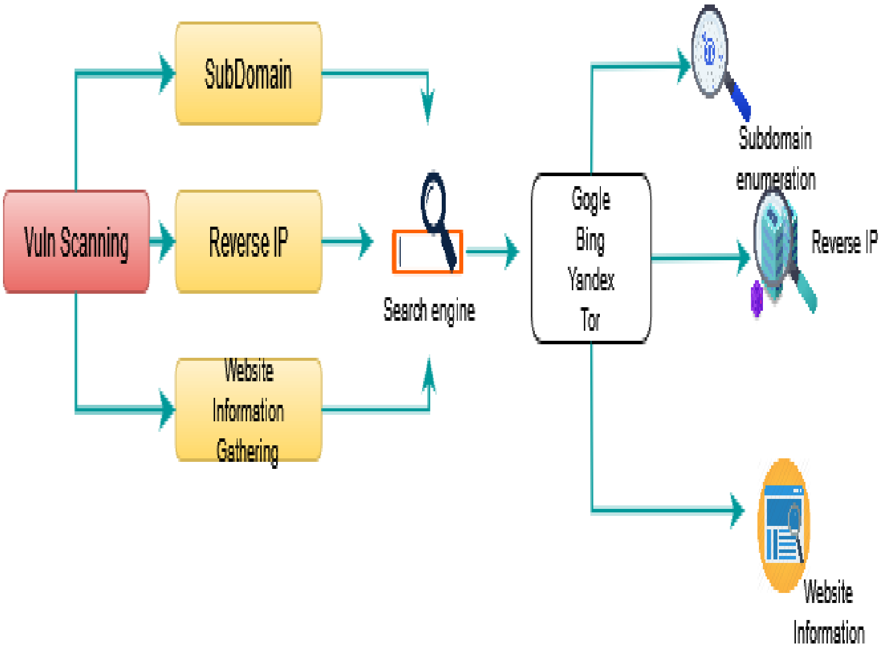


Figure 3. Website Vulnerability Scanning

In the website vulnerability scanning phase, this tool contains options are:

- **Subdomain Enumeration**

  Subdomain enumeration is the process of finding valid subdomains for one or more domains.
- **Reverse IP**

  Reverse IP lookup also known as reverse DNS lookup, is the process of querying the DNS to determine the domain name associated with an IP address.
- **Website Information Gathering**

  Finding website information like DNS servers, IP addresses, mail servers, SPF information, open ports, host IP, hostname, internet number, net name, name server, registry domain id, creation date, updated date, registry expiry date, and admin information, etc.

4.3 Network Scanning-Network Scanning is the procedure of identifying active hosts, ports, and services used by the target application.

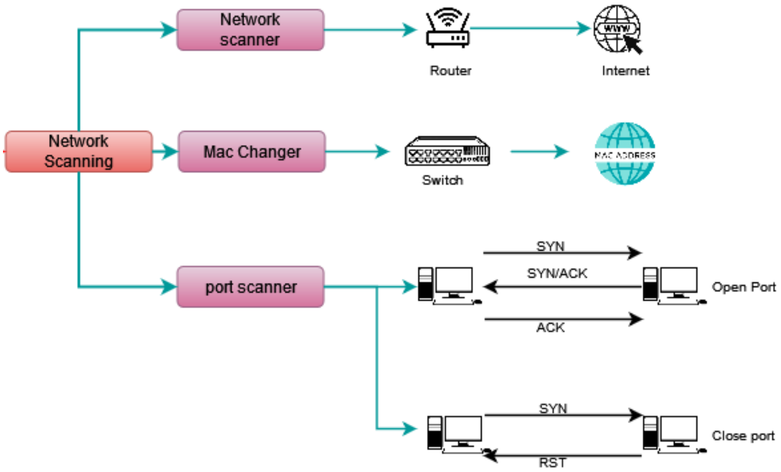


Figure 4. Network Scanning Diagram

Network Scanning phase this tool contains options are:

- **Network Scanner**

  Network scanning helps to discover any live computer or hosts, open ports, and the IP address of a victim. Network scanning helps to find out the vulnerabilities and threats in the network.

- **Mac Changer**

  MAC Changer is a utility that makes the manipulation of MAC addresses of network interfaces easier.

- **Port Scanning**

  A port scan is a method for determining which ports on a network are open. A port scan is a common technique hackers use to discover open doors or weak points in a network.

4.4 Bug Bounty Tool-A bug hunt is a robust explorative test that finds bugs and vulnerabilities in websites or mobile apps

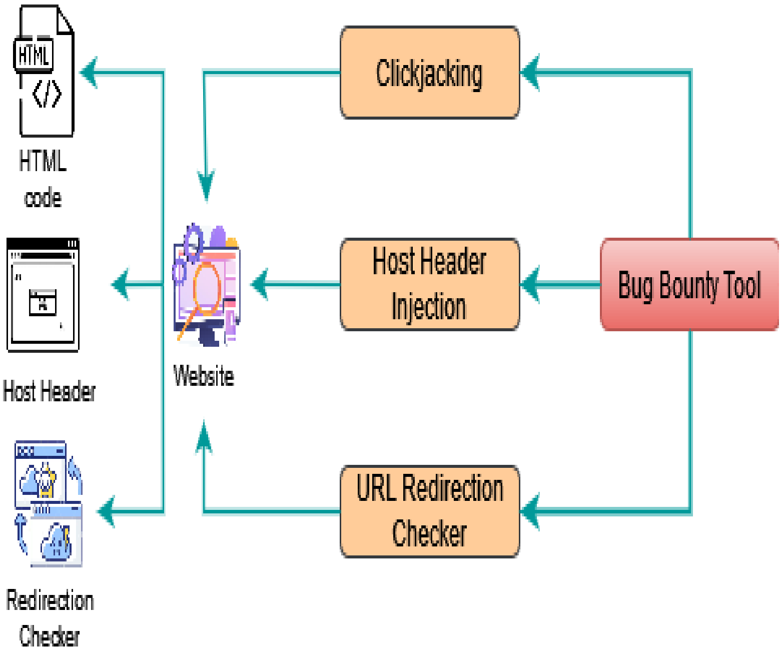


Figure 5 Bug Bounty Tool Diagram

In the Bug Bounty phase, this tool contains options are:

- **Click Jacking**

  It has the option for finding outing click jacking vulnerabilities in websites. Click jacking is an attack that tricks a user into clicking a web page element that is invisible or disguised as another element.

- **Host Header Injection**

  It has the option for finding outing Host Header Injection vulnerabilities in websites. Host header injection is an attack in which a malevolent actor tampers with the host header in a client request

- **URL Redirection Checker**

  It has the option for finding outing URL Redirection vulnerabilities in websites. URL redirection also called URL forwarding is a World Wide Web technique for making a web page available under more than one URL address. When a web browser attempts to open a URL that has been redirected, a page with a different URL is opened.

4.5 Anatomy of URL-URL stands for Uniform Resource Locator. A URL is nothing more than the address of a given unique resource on the Web.

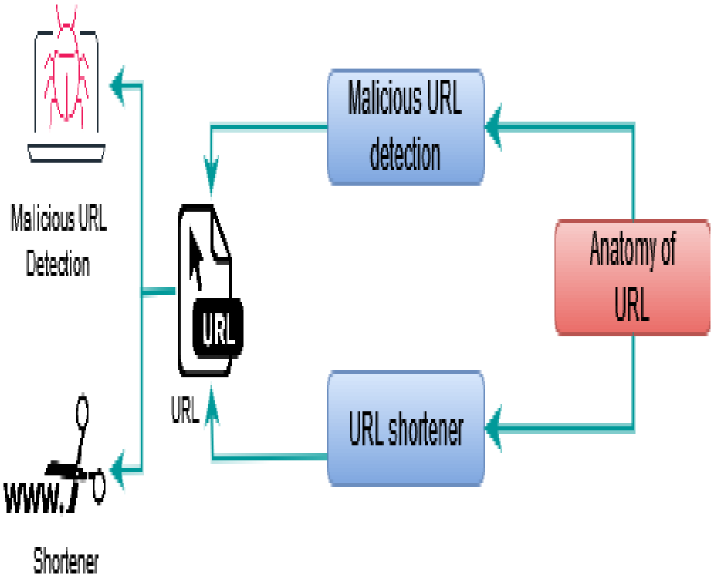


Figure 6. Anatomy of URL Diagram

In the Anatomy of URL phase, this tool contains options are:

- **Malicious URL Detection**

  The technology of malicious URL detection can help users identify malicious URLs and prevent users from being attacked by malicious URLs. Also, users get more details about URLs like IP address, server, content type, status code, page size, spamming, malware, phishing, suspicious, risk score, category, etc.

- **URL Shortener**

  A URL shortener is a tool that creates a short, unique URL that will redirect to the specific website of your choosing.

4.6 Payload Generator

It has the option for generating payloads for different kinds of a platform like Windows, Linux, iOS, Python, PHP, and Java. Payloads are malicious scripts that an attacker uses to interact with a target machine to compromise it. A payload is a piece of code that executes when hackers exploit vulnerability. In other words, it's an exploit module.

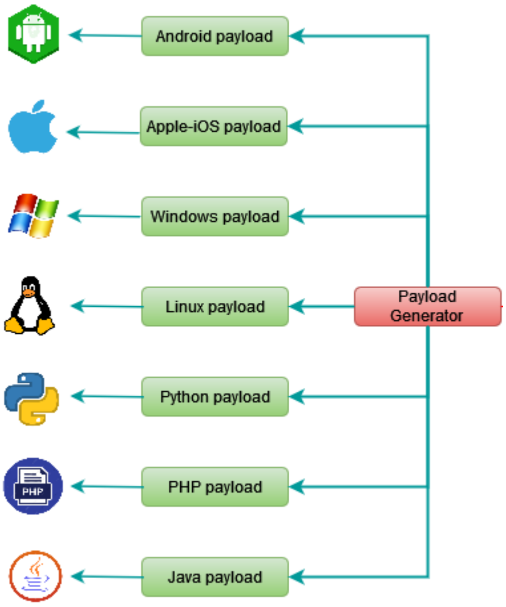


Figure 7. Payload Generator Diagram

In the Payload Generator phase, this tool contains options are:

- **Android Payload Generator**

  Used to create payload for android devices, the payload in application format.
- **Apple-iOS Payload Generator**

  Used to create payload for apple-iOS devices, the payload in iOS format.
- **Windows Payload Generator**

  Used to create payload for windows devices, the payload in executable format.
- **Linux Payload Generator**

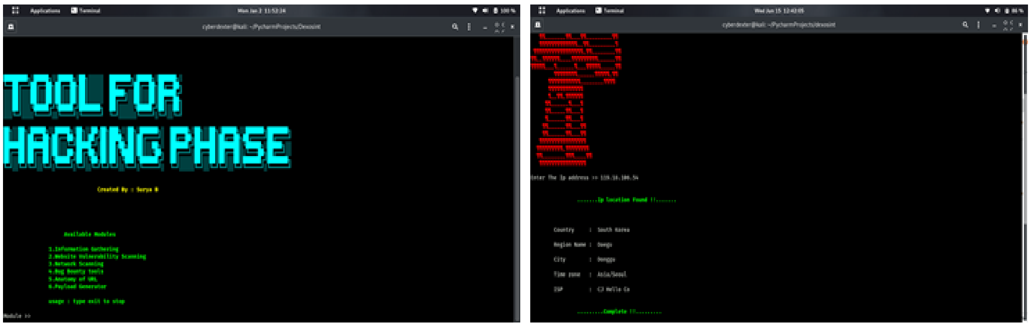
  Used to create payload for Linux devices, Executable and Linkable Format in application format.
- **Python Payload Generator**

  Used to create payload for python-based devices, the payload in python format.
- **PHP Payload Generator**

  Used to create payload for PHP-based devices, the payload in PHP format.
- **Java Payload Generator**

  Used to create payload for windows devices, the payload in a jar or JDK format.

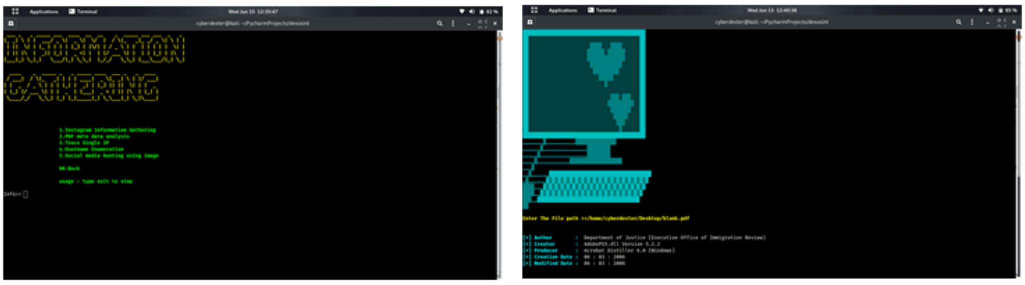
5. Screen Shots


Applications
Terminal
cyberdexter@kali: ~/PycharmProjects/Dexosint
Applications
Terminal
cyberdexter@kali: ~/PycharmProjects/dexosint

```
TOOL FOR
HACKING PHASE

              Created By : Surya R


          Available Modules

        1.Information Gathering
        2.Website Vulnerability Scanning
        3.Network Scanning
        4.Bug Bounty tools
        5.Anatomy of URL
        6.Payload Generator

        usage : type exit to stop
Module >>
```

```
Enter The Ip address >> 119.16.186.54

          .......Ip Location Found !!.......


     Country     :  South Korea

     Region Name :  Daegu

     City        :  [illegible]

     Time zone   :  Asia/Seoul

     ISP         :  CJ Hello Co

          ........Complete !!........
```

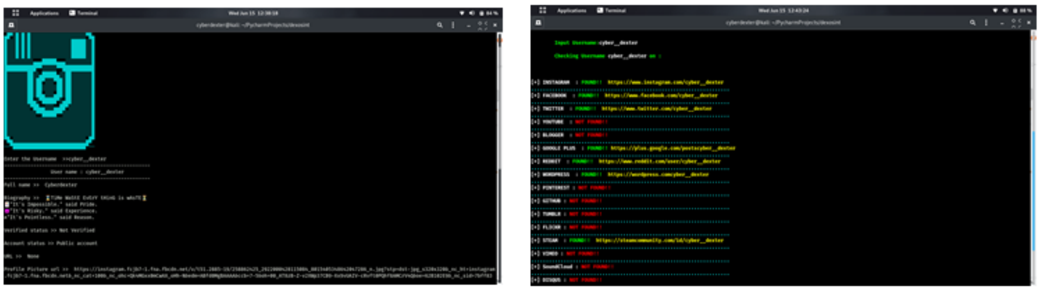
Figure 8 . Home Page and Trace IP Diagram



```
INFORMATION
GATHERING

        1.Instagram Information Gathering
        2.PDF meta data analysis
        3.Trace Single IP
        4.Username Enumeration
        5.Social media hunting using image

        00.Back

        usage : type exit to stop

Info>>
```

```
Enter The File path >>/home/cyberdexter/Desktop/blank.pdf

[+] Author        :  Department of Justice (Executive Office of Immigration Review)
[+] Creator       :  AdobePS5.dll Version 5.2.2
[+] Producer      :  Acrobat Distiller 6.0 (Windows)
[+] Creation Date :  06 : 03 : 2006
[+] Modified Date :  06 : 03 : 2006
```

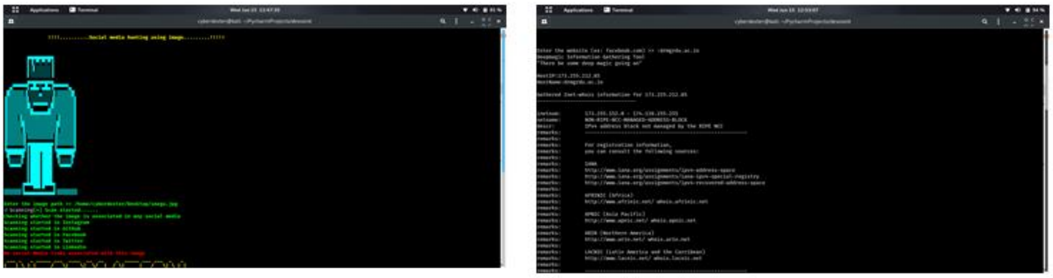
Figure 9. Information Gathering Diagram and PDF Metadata Analysis Diagram



```
Enter the Username  >>cyber__dexter
------------------------------------------
            User name : cyber__dexter
------------------------------------------
Full name >>  CyberDexter

Biography >>  [illegible]
'It's Impossible.' said Pride.
'It's Risky.' said Experience.
'It's Pointless.' said Reason.

Verified status >> Not Verified

Account status >> Public account

URL >>  None

Profile Picture url >>  https://instagram.[illegible]
```

```
     Input Username:cyber__dexter

     Checking Username cyber__dexter on :

[+] INSTAGRAM  : FOUND!!  https://www.instagram.com/cyber__dexter
[+] FACEBOOK  : FOUND!!  https://www.facebook.com/cyber__dexter
[+] TWITTER  : FOUND!!  https://www.twitter.com/cyber__dexter
[+] YOUTUBE  : NOT FOUND!!
[+] BLOGGER  : NOT FOUND!!
[+] GOOGLE PLUS  : FOUND!! https://plus.google.com/postscyber__dexter
[+] REDDIT  : FOUND!!  https://www.reddit.com/user/cyber__dexter
[+] WORDPRESS  : FOUND!!  https://wordpress.com/cyber__dexter
[+] PINTEREST : NOT FOUND!!
[+] GITHUB : NOT FOUND!!
[+] TUMBLR : NOT FOUND!!
[+] FLICKR : NOT FOUND!!
[+] STEAM  : FOUND!!  https://steamcommunity.com/id/cyber__dexter
[+] VIMEO : NOT FOUND!!
[+] SoundCloud : NOT FOUND!!
[+] DISQUS : NOT FOUND!!
```

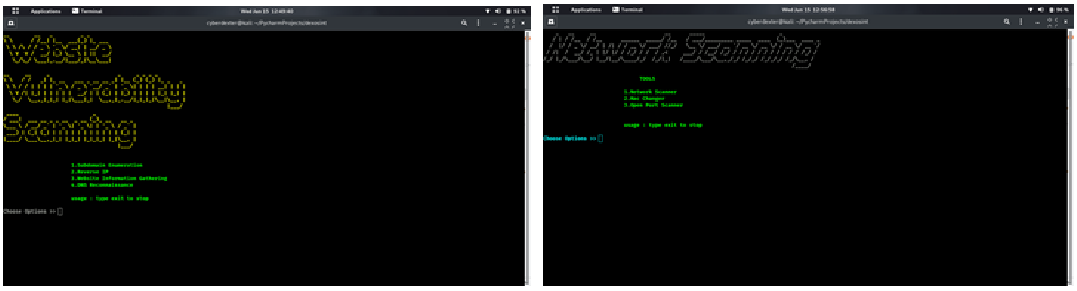
Figure 10. Instagram Information Gathering Diagram and Username Enumeration Diagram



```
     !!!!..........Social media hunting using image..........!!!!!

Enter the image path >> /home/cyberdexter/Desktop/image.jpg
[illegible] Scan started......
Checking whether the image is associated to any social media
Scanning started in Instagram
Scanning started in GitHub
Scanning started in Facebook
Scanning started in Twitter
Scanning started in LinkedIn
No social Media [illegible] with this image
```

```
Enter the website (ex: facebook.com) >> [illegible]
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:[illegible]
HostName:[illegible]

Gathered Inet-whois information for [illegible]
---------------------------------

inetnum:        [illegible]
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        ------------------------------------------------
remarks:
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:
remarks:        LACNIC (Latin America and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks:        ------------------------------------------------
```

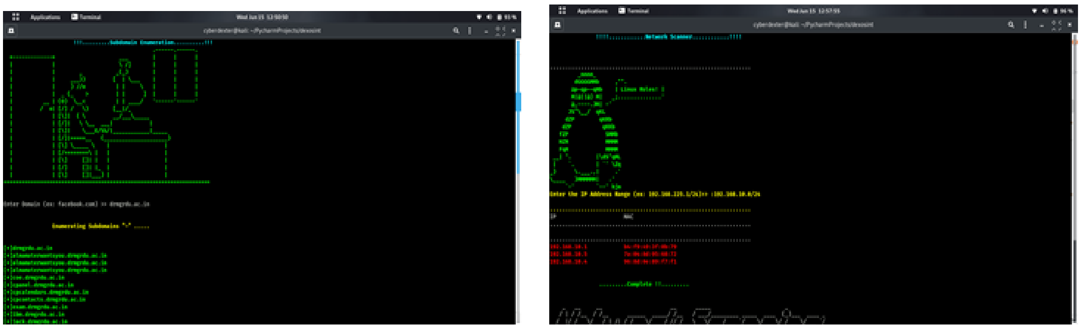
Figure 11. Social Media Hunting using Image Diagram and Website Information Gathering Diagram



```
Website
Vulnerability
Scanning

        1.Subdomain Enumeration
        2.Reverse IP
        3.Website Information Gathering
        4.DNS Reconnaissance

        usage : type exit to stop

Choose Options >>
```

```
Network Scanning

             TOOLS

          1.Network Scanner
          2.Mac Changer
          3.Open Port Scanner

          usage : type exit to stop

Choose Options >>
```

Figure 12. Website Vulnerability Scanning Diagram and Network Scanning Diagram



```
     !!!!..........Subdomain Enumeration..........!!!

Enter Domain (ex: facebook.com) >> [illegible]

        Enumerating Subdomains "*" ......

[illegible]
```

```
     !!!!..........Network Scanner..........!!!!

                    | Linux Rules! |

Enter the IP Address Range (ex: [illegible]) >> [illegible]
------------------------------------------------------------
IP                  MAC
------------------------------------------------------------
[illegible]         [illegible]
[illegible]         [illegible]
[illegible]         [illegible]

        ........Complete !!.........
```

Figure 13. Subdomain Enumeration Diagram and Network Scanner Diagram

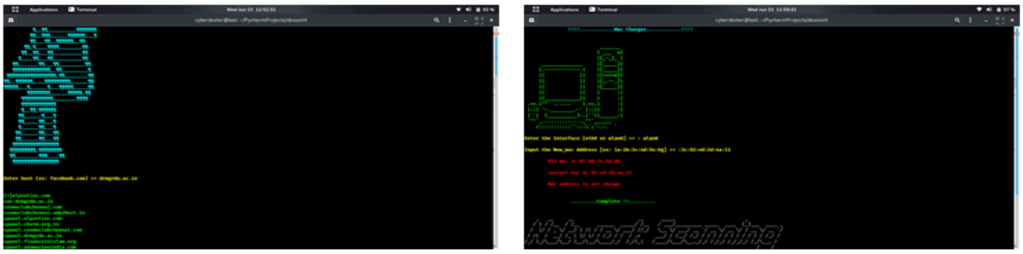


Figure 14. Reverse IP Diagram and Mac Changer Diagram

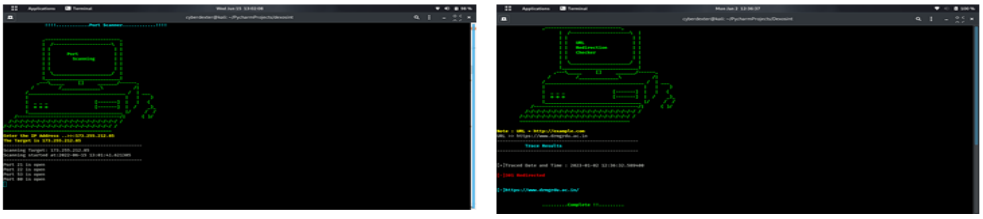


Figure 15 .Port Scanning Diagram and URL Redirection Checker Diagram

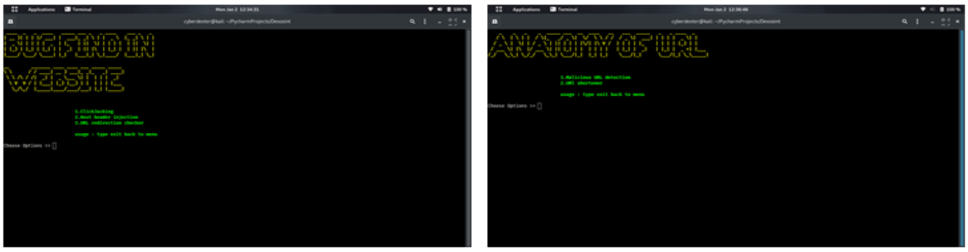


Figure 16. Bug Bounty Tool Diagram and Anatomy of URL Diagram

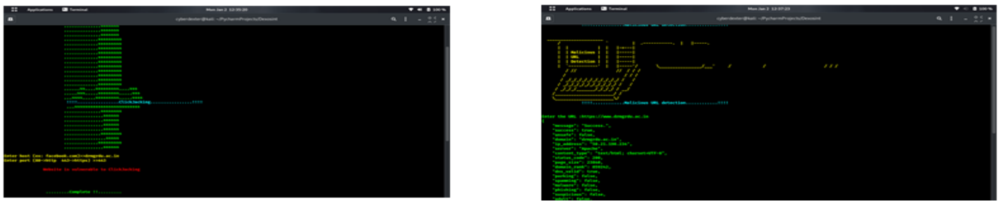


Figure 17. Click Jacking Diagram and Malicious URL Detection Diagram

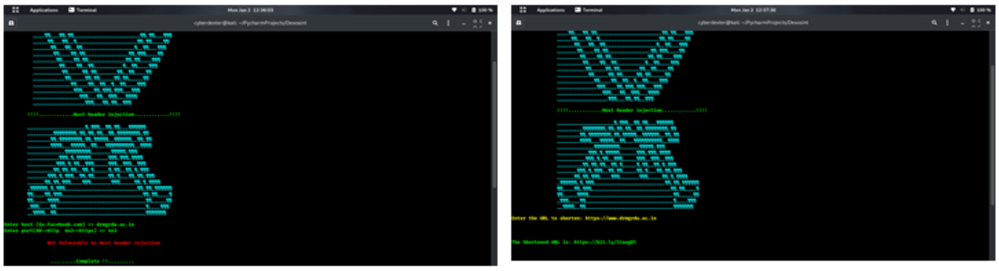


Figure 18. Host Header Injection Diagram and URL Shortener Diagram

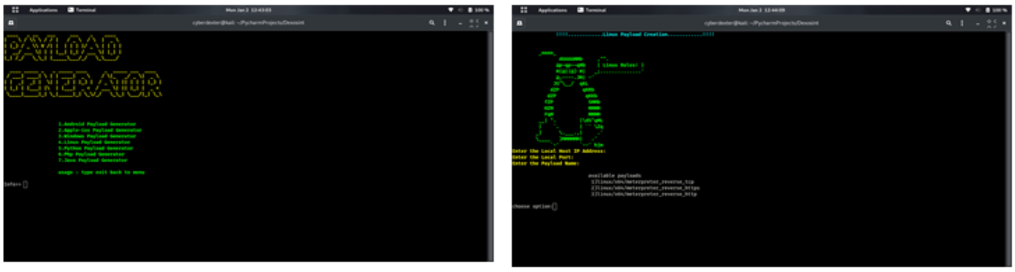
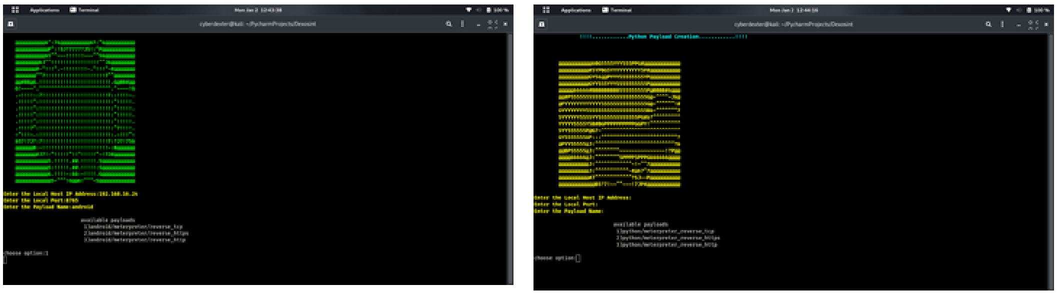


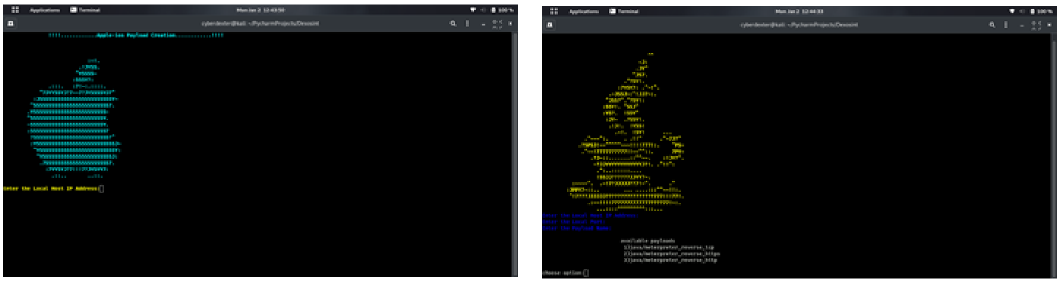
Figure 19. Payload Generator Diagram and Linux Payload Generator Diagram



```
Enter the Local Host IP Address:192.168.16.2
Enter the Local Port:8765
Enter the Payload Name:android

                    available payloads
                     1)android/meterpreter/reverse_tcp
                     2)android/meterpreter/reverse_https
                     3)android/meterpreter/reverse_http

Choose option:1
```

```
      !!!!...........Python Payload Creation...........!!!!

Enter the Local Host IP Address:
Enter the Local Port:
Enter the Payload Name:

                    available payloads
                     1)python/meterpreter_reverse_tcp
                     2)python/meterpreter_reverse_https
                     3)python/meterpreter_reverse_http

Choose option:
```

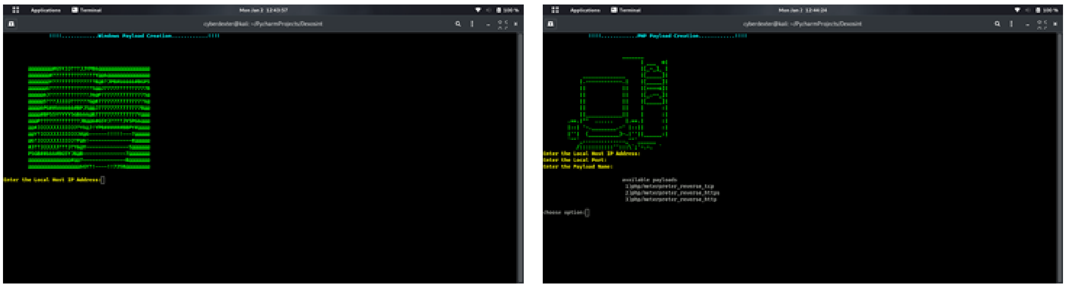
Figure 20. Android Payload Generator Diagram and Python Payload Generator Diagram



```
      !!!!...........Apple-ios Payload Creation...........!!!!

Enter the Local Host IP Address:
```

```
Enter the Local Host IP Address:
Enter the Local Port:
Enter the Payload Name:

                    available payloads
                     1)java/meterpreter_reverse_tcp
                     2)java/meterpreter_reverse_https
                     3)java/meterpreter_reverse_http

Choose option:
```

Figure 21. Apple iOS Payload Generator Diagram and Java Payload Generator Diagram



```
      !!!!...........Windows Payload Creation...........!!!!

Enter the Local Host IP Address:
```

```
      !!!!...........PHP Payload Creation...........!!!!

Enter the Local Host IP Address:
Enter the Local Port:
Enter the Payload Name:

                    available payloads
                     1)php/meterpreter_reverse_tcp
                     2)php/meterpreter_reverse_https
                     3)php/meterpreter_reverse_http

Choose option:
```

Figure 22. Windows Payload Generator Diagram and PHP Payload Generator Diagram

III. CONCLUSIONS

The main purpose of this project is to facilitate the work of Ethical hackers. Ethical hacking is a process of detecting vulnerabilities in an application, system, or organization's infrastructure. This tool very helps full for ethical hackers with penetration testing on systems or networks. There are mainly 5 phases in hacking. Not necessarily a hacker has to follow these 5 steps sequentially. It's a step-wise process and when followed yields a better result. This tool has the tools needed for Ethical hacking phases like reconnaissance, scanning, gaining access, maintaining access, and clear tracking. So this tool makes ethical hacker work easier. We have got good results from these modules.

IV. REFERENCES

[1] Vijaya R Saraswathi, Iftequar Ahmed Sk, Sriveda Reddy M, Vrushik Reddy M, Sanjana Reddy M. Automation of Recon process for Ethical Hackers", Year: 2022.

[2] Aswathy Mohan, G Aravind Swaminathan, N. Jeenath Shafana, "Automated Tools and Techniques in Vulnerability Assessment", Year: 2022.

[3] Sushmita Reddy Mamilla, "A Study of Penetration Testing Processes and Tools", Year: 2021.

[4] R. Sri Devi, M. Mohan Kumar, "Testing for Security Weakness of Web Applications using Ethical Hacking", Year: 2020.

[5] Sudhanshu Raj, Navpreet Kaur Wali, "A Study on Metasploit Framework: A Pen-Testing Tool", Year: 2020.