Manoj Saha al. 2022, 10:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science,
Engineering and Technology

An Open Access Journal

Information Gathering of Ethical Hacking using Reconnaissance Framework

Manoj Saha, Vijayakumar Adaickalam
Dept. of Computer Science and Information Technology
Jain Deemed-to-be University, Bengaluru, India

Abstract- In Global Cybersecurity Outlook 2022 report it has pointed that due to Covid-19 Pandemic has increase the rate of online transaction and cybercrimes. Technology has evolved rapidly and have become the essential part of life. Due to pandemic everything has been shifted to online mode for safety precautions but it has led to high cybercrimes throughout the world. According to the researcher, professional who work from home have high possibility of being the next victims. It is important and right time to know about how hacker works, which tools does the hacker use and behavior. The success of ethical hacking depends on the data and information gathered during the phase of reconnaissance, which technically means gathering information about the possible target. Reconnaissance is a very vast process which can be carried out by different tools but not together, every tool works separately which creates lot of work heads and time consuming. In this proposed work, a program is built with python programming language which provide the functionality of live network capturing, port scanning, domain information, clickjacking testing and many more features. It gives the idea of how general information can be effectively protected against the possible attacks.

Keywords-Capturing, Clickjacking, Cybercrime, Domain, Ethical Hacking Reconnaissance, Technology

I. INTRODUCTION

As in step with the World Economic Forum's Global Risks Report 2021, cyber dangers maintain rating among worldwide dangers. The COVID-19 pandemic has multiplied technological adoption, but uncovered cyber vulnerabilities and unpreparedness, whilst on the identical time exacerbated the tech inequalities inside and among societies. Looking on the year ahead, it's far important to maintain raising cybersecurity as a strategic commercial enterprise trouble and increase greater partnerships among industries, commercial enterprise leaders, regulators and policymakers.

Organizational priorities have to consist of a proactive plan for every commercial enterprise to construct and hold its own cybersecurity workforce. With protection information turning into so hard to supply and retain, companies have to keep in mind cultivating this expertise organically. Organizations period advantages as a way to accrue from a popularity for cultivating this information, transmitted from veterans to learners getting into the field. We have discovered plenty during the last 18 months, and 2021 can be no different. We want to maintain to adapt and take cyber dangers significantly with the aid of using planning, getting ready and educating. Since it's far a usual trouble, open communications among corporations, policymakers, and regulators are a important key to success.

Until protection functions grow to be indispensable to generation – seamless, transparent, and clearly usable with the aid of using people. When it involves cybersecurity, a framework serves as a gadget of standards, guidelines, and best practices to manipulate dangers that rise up in a virtual world. A cybersecurity framework prioritizes a flexible, repeatable and cost-powerful technique to sell the safety and resilience of your commercial enterprise.

It's vital to recognize that cybersecurity facilitates with the increase of your commercial enterprise. Using a framework to align controls like local, offline, and cloud backups will enhance resilience from any assault or reliance on hardware. As an MSP, the more paintings of constructing out a system will fall onto you, however will permit you to maintain your customers responsible and vice versa.

- In the present gadget, I actually have found that ethical hacker is operating with different types of reconnaissance tools, one at a time in Debian or Arch running gadget environment, which can create lot of workload and complexity.
- In present gadget, I actually have studied the studies papers and discovered out that we've very beneficial device which can used for data accumulating like Nmap, traceroute, and whois and DNS
- In present gadget, there may be loss of framework wherein we don't capable of wherein we will see the usage of various open supply device in a single platform.

Why Use the Cybersecurity Framework?
The Framework gives systematic method for handling cybersecurity danger. The Core consists of sports to be included in a cybersecurity application that may be tailor-made to meet any agency's needs. The Framework is designed to complement, now no longer replace, an agency's cybersecurity application and danger control processes.

What is the Impact of Cybercrime?
A loss of awareness on cybersecurity can harm your commercial enterprise in variety of approaches including:

Economic Costs: Theft of highbrow property, company data, disruption in buying and selling and the cost of repairing broken systems Reputational Cost: Loss of purchaser trust, lack of modern and destiny clients to competition and poor media coverage

Regulatory Costs: GDPR and different information breach legal guidelines suggest that your agency should go through from regulatory fines or sanctions due to cybercrimes. All businesses, no matter the size, should make certain all personnel apprehend cybersecurity threats and the way to mitigate them. This have to consist of normal schooling and a framework to paintings with to that goals to reduce the danger of information leaks or information breaches. Given the character of cybercrime and the way hard it may be to detect, it's far hard to apprehend the direct and oblique fees of many protection breaches. This doesn't suggest the reputational harm of even a small information breach or different protection occasion isn't large. If anything, customers anticipate an increasing number of state-of-the-art cybersecurity measures as time is going on

II.RELATED WORK

- Wojciech Mazurczyk and Luca Caviglione (1) have proposed that it has focused on the reconnaissance phase, which is the basis for the totality of cybersecurity attacks. Engineer a new-wave of reconnaissance-proof-by design services, for instance, by minimizing the impact of the addressing scheme, the use of IoT and the exposition to scanning services like Shodan and re-think the concept of privacy in a broader manner to also include protection mechanisms against advanced and malicious data gathering campaigns.

- Shanto Roy, Nazia Sharmin, Jamie C. Acosta, Christopher Kiekintveld and Aron Laszk (2) have proposed one of the main lessons is the overall scope and diversity of the problem of adversarial reconnaissance in cybersecurity. The variety of types of information that could potentially be useful to an attacker is vast, as is the number of tools and specific techniques for obtaining it. This is also a moving target, as the types of information that are relevant and the tools will naturally evolve over time with technology.
- Danda B. Rawat (3) have proposed that the cyber defense teams to leverage data-driven techniques with AI for cybersecurity, where AI learns and enhances its knowledge base more quickly to better detect, predict and respond to cyber-attacks. The results have revealed that the probability of cyber-attack decreases as the education and income level of victim increases. It is believed that cyber-crime units will use the proposed model. It will also facilitate the detection of cyber-attacks and make the fight against these attacks easier and more effective in near future.
- Abdulkadir Bilen and Ahmet Bedri Azur (4) proposed that, it analyses the cyber-crimes in two different models with machine-learning concept and predicted the effect of the defined features on

the detection of the cyber-attack methods and the perpetrator behavior and actions.

- Ahmad Mtair AL Hawamleh, Alorfi Almuhannad Sulaiman M, Jassim Ahmad Al-Gasawneh, and Ghada Al-Rawashdeh (5) proposed about the importance of cybersecurity and the use of ethical hacking techniques for user data protection through the characterization of globally established standards and techniques for organizations to apply, in the prevention of likely cyber threats while assuring user data protection.
- Rohit Kalakuntla, Anvesh Babu Vanamala and Ranjith Reddy Kolipyaka (6) proposed about the motivation, behaviour and countermeasure behind the cyber security and cyber terrorism. Cyber Security accepts a vigorous role in the area of information technology. Safeguarding the information has become an enormous problem in the current day. The cybersecurity the main thing that originates in mind is 'cyber crimes' which are aggregate colossally daily. Different governments and organizations are taking numerous measures to keep these cyber wrongdoings.
- Idimadakala Nagaraju (7) proposed about the ethics of using cybersecurity tool and understanding the true intentions of every single ethical hacker getting into vulnerable systems or networks. Technology is ever growing and people are encountering tools that are beneficial to them. If these tools fall into the wrong hands they can create great controversy, breaching our basic right to privacy, respect and freewill. The constant issues highlighted by the media always reporting some type of cyber-crime, a study showing that nearly 93% of attacks happened inside of the organization raising concerns of how easy it is to be working inside to be able to infiltrate attacks.
- Saloni Khurana (8) proposed about the exploration on how cybercrime has become a serious threat in our lives and it highlight are some of the different security methods that are being used in malicious approaches, techniques and attack and their various loopholes.
- Pavan Kumar and K. Pranathi (9) proposed that the entire world is moving toward technological advancements and increasing digitization of real-world operations, which raises the risk of security. The workings of malicious hackers or crackers, on the one hand, who try to illegally break into security, and white hat hackers or ethical hackers, on the other hand, who try to preserve security and trying harden the security configuration and patching critical vulnerabilities.
- Brijesh Kumar Pandey, Alok Singh and Lovely lakhmani Balani (10) have proposed about the concepts of system security, hacking, hacker, ethical hacking aka pen testing. Then in next section it discussed about various tools, techniques and approaches which are normally constitutes weaponry of a seasoned hacker and their behavioral mindset. It also explains it has explained how ethical hacking is a continuous and dynamic process, then it discussed various opportunities available to an ethical hacker as a professional.

III.PROPOSED SYSTEM

The core objective of the study is to create a proper framework, where we can gather information about target IP, domain, port, technologies and other related topics.

It has incorporated graphical network monitor and packet sniffer along with reconnaissance. To frame the proposed work, I have tried to incorporate different types of open source reconnaissance tool into one environment. This challenge aims to feature-wise functions like Clickjacking, additionally referred to as a “UI redress assault” which is an interface-primarily based totally assault wherein a person is tricked into clicking on the actionable content material on a hidden website via way of means of clicking on a few different content materials in a decoy internet site.

Reconnaissance is a vital device for penetration trying out and the start factor of many information breaches. The procedure entails amassing statistics approximately the goal system, that would be used to discover flaws and vulnerabilities. In the reconnaissance stage, attackers act like detectives, amassing statistics to virtually recognize their goal. The element is everything! From inspecting electronic mail lists to opening supply information, their aim is to recognize the network higher than the individuals who run and keep it. They hone in on the security component of the technology, have a look at the weaknesses, and use any vulnerability to their advantage.

Reconnaissance can be divided into two phases:

1. Passive reconnaissance.: In this section, a pentester attempts to accumulate records approximately the

goal, via publicly available sources, one such supply is Open-source intelligence also regarded as (OSINT). There are many different sources like Shodan that are very effective gear in terms of passive reconnaissance.

2. Active reconnaissance: In this method, you may directly engage with the laptop machine to benefit data. These records may be relevant and accurate. But there may be a chance of getting detected in case you are making plans for lively reconnaissance without permission. If you're detected, then the machine admin can take severe action against you and trail your next activities.

IV.FOOTPRINTING, SCANNING, AND ENUMERATION

The method of reconnaissance may be done via way of means of Footprinting, Scanning, and Enumeration. These three are the subprocess of reconnaissance that allows us to accumulate powerful records from the host or the target.

Foot printing is the method of accumulating a lot of records as viable approximately a target network, for locating numerous approaches to intervene into an organization's community machine. Once you methodologically start the foot printing method, you may acquire the blueprint of the safety profile of the target organization. The term "blueprint" is used right here due to the fact that the end result accumulated on the give-up refers back to the particular machine profile of the target organization

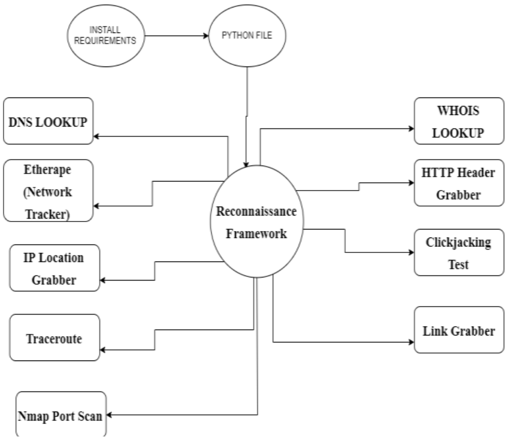


Fig 1 Proposed System

3.1 Python Programming Language

Python is a flexible programming language for both teaching machines to learn and for analyzing extensive amounts of data. Python is one of the best programming languages for AI creation. Choose it because of its simple syntax, a wide variety of frameworks with hundreds of source codes, and a supportive user system for beginners. Data scientists should practice analyzing information with Python since it simplifies the complicated process of interpreting data, detecting important insights, and generating predictions. The creation of bots, desktop, web, and game development is also one of the examples of what Python is used for.

3.2 Etherape

EtherApe is a graphical network traffic tarcker display for Unix modelled after Etherman. Featuring hyperlink layer, IP and TCP modes, it shows network activity graphically. Hosts and hyperlinks alternate in size with traffic. Colour-coded protocols display. It supports Ethernet, FDDI, Token Ring, ISDN, PPP, SLIP and WLAN devices, plus numerous encapsulation formats. It can help clear out traffic to be shown and might examine packets from a file, in addition, live from the network. Plug it into the control or span port of your switch and get a real-time graphical flow of what's taking place for your community network.

3.3 DNS Lookup

The simple concept of DNS is that people can't easily recollect long strings of digits like machines can, however, can be much more effortlessly recalled words. So, when you type a website like www.techopedia.com, the request is forwarded to a DNS server (whether or not domestically or at an ISP), which returns the corresponding IP address. This address is then utilized by all of the computer systems and routers to channel the request and responses of a person's specific session. The end result is that the person sees internet pages as anticipated or has email displayed up in an in-box. The kinds of DNS lookups are forward DNS lookups and reverse DNS lookups

3.4 WHOIS lookup

whois searches for an object in a whois database. whois is a query and response protocol that is widely used for searching databases that present users from an internet source, such as a domain name of an IP address. As part of the domain registration process, registrants must provide their registrar with correct and dependable contact details and make sure this information is kept up to date. Failing to provide reliable information, or a willful failure to replace out of date data supplied to a registrar can lead to your registration being canceled. The registrar that you pick will ask you to offer contact and technical records, some of which are required by ICANN (The Internet Corporation for Assigned Names and Numbers). Personal data such as e-mail addresses etc. can be included in a WHOIS result.

3.5 NMAP Port Scan

Nmap is a community network mapper that has emerged as one of the most popular, free network discovery equipment on the market. Nmap is now one of the middle pieces of equipment utilized by community network directors to map their networks. The application may be used to discover stay hosts in a network, carry out port scanning, ping sweeps, OS detection, and model detection.

A variety of new cyberattacks have re-targeted interest in the kind of community network auditing that Nmap provides. Analysts have talked about that the latest Capital One hack, for instance, might have been detected faster if machine directors were tracking linked devices. Nmap is the maximum used device for scanning open ports. Naturally, Nmap can do a whole lot greater than that. Nmap ("Network Mapper") is an open-supply device for community exploration and protection auditing. In the device, the Nmap scans the desired hyperlink or IP cope with and searches for open ports. A Nmap -Pn experiment is used withinside the Reconnaisance script. Pn is used to deal with all hosts as an line bypass host discovery

3.6 Clickjacking

Clickjacking additionally called a “UI redress assault” is an interface-primarily based totally attack wherein a consumer is tricked into clicking on the actionable content material on a hidden internet site with the aid of a user clicking on a few different contents in a decoy website.

In easy words, an attacker makes use of a couple of obvious or opaque layers to trick a consumer into clicking on a button or hyperlink on any other web page once they have been proceeding to click on the top-level web page. Thus, the attacker is “hijacking” clicks intended for his or her web page and routing them to any other web page, most possibly owned with the aid of using any other application, domain, or both. Using a comparable technique, keystrokes also can be hijacked. With a cautiously crafted combination of stylesheets, iframes, and textual content boxes, a consumer may be caused to trust they're typing withinside the password to their e-mail or financial institution account, however, are as an alternative typing into an invisible body controlled by the attacker. Clickjacking is an attack when an attacker uses a transparent iframe in a window to trick a user into dicking on button or link to another server in which they have an identical looking window. The attacker in a sense hijacks the dicks meant for the original server and sends them to the other server.

X-Frame-Options is an HTTP response header, also referred to as an HTTP security header. This header tells your browser how to behave when handling your site's content. X-Frame Options are used to indicate whether the browser can render a page in an iframe frame or object. The three possible values are:

- DENY. The page cannot be rendered in a frame under any circumstance.
- SAMEORIGIN. The page can only be displayed in a frame it the "framing site is on the same origin.
- ALLOW FROM: The page can only be framed from a specific origin.

3.7 Http Grabber

The HyperText Transfer Protocol (HTTP) is a consumer server protocol powering most of the internet. Every time you surf the internet, your browser sends HTTP requests for HTML pages, images, scripts, and CSS. Web servers manage those requests through returning responses containing the asked useful resource, for this reason completing the HTTP request-reaction cycle. HTTP headers allow the consumer and the server to pass extra data with an HTTP request or response.

An HTTP header includes its case-insensitive call accompanied through a colon (:), then through its cost. Whitespace earlier than the value is ignored. Custom proprietary headers have traditionally been used with an X- prefix, however, this convention became deprecated in June 2012 due to the inconveniences it caused when nonstandard fields have become widespread in RFC 6648; others are indexed in an IANA registry, whose authentic content material became described in RFC 4229. IANA additionally keeps a registry of proposed new HTTP headers. Headers may be grouped consistent with their contexts:

- Request headers comprise more data about the resource to be fetched, or approximately the consumer asking for the useful resource.
- Response headers keep extra data approximately the reaction, like its vicinity or approximately the server presenting it.
- Representation headers comprise data approximately the frame of the useful resource, like its MIME type, or encoding/compression applied.
- Payload headers comprise representation-impartial data approximately payload data, consisting of content material duration and the encoding used for transport.

3.8 Link Grabber

Internal and outside hyperlinks may be displayed with this records-gathering device.

When security testing an organization or internet site, forgotten and poorly maintained internet packages can be a tremendous area to locate susceptible spots. Dumping the web page hyperlinks is a short manner to locate different related packages, internet technologies, and associated websites. The HTML is then analyzed, and URLs are extracted from the results. This method is referred to as scraping.This device lets in a quick and clean manner to scrape hyperlinks from an internet web page. Listing hyperlinks, domains, and assets that a web page hyperlinks to inform you loads approximately the web page. Reasons for the usage of a device consisting of this are wide-ranging from Internet research, internet web page improvement to security assessments, and web page testing.

3.9 Ip Location Finder

IP geolocation is the mapping of an IP address to the geographic area of the internet from the related device. By geographically mapping the IP address, it gives you area facts along with the country, state, city, zip code, latitude/longitude, ISP, location code, and different facts. ARIN's WHOIS provider offers contact and registration facts for the IP research and free access. When an enterprise acquires a block of IP addresses, a request is submitted after which the IPs are assigned to the asked ISP. The IP geolocation information receives up to date routinely primarily based totally on the databases of the nearby Internet registry (RIR). Manual updates aren't possible. There are many extraordinary IP area databases wherein you may pull from. Most providers declare a 98% or better accuracy. IP mapping to unique towns can on occasion range barely primarily based totally upon the area of the closest ISP provider's community hub**.**

3.10 Traceroute

As the name suggests traceroute, is a method of tracing the route. Traceroute is a twork-based application that suggests the route over the community network among structures and lists all of the intermediate routers to get to the final destination. The predominant reason for traceroute is to repair community network problems. This enables you in figuring out while connecting to a few communities network wherein the relationship is truly slowing down, which intermediate router is answerable for that. Using the internet to connect with anything really is now no longer for your nearby network or handled by your net provider traceroute tracks the direction packets taken from an IP community on their manner to a given host. It makes use of the IP protocol's time to live (TTL) discipline and tries to elicit an ICMP TIME EXCEEDED reaction from every gateway alongside the route to the host When reviewing your results, you will see the subsequent statistics for the route

- The number of route.
- The quantity of time it took for each of the 3 attempts in milliseconds.
- The IP address of the node at that hop.
- The domain name is available.

V. RESULTS AND DISCUSSION

1.Data flow Diagram

This diagram explains how the control moves in the proposed System

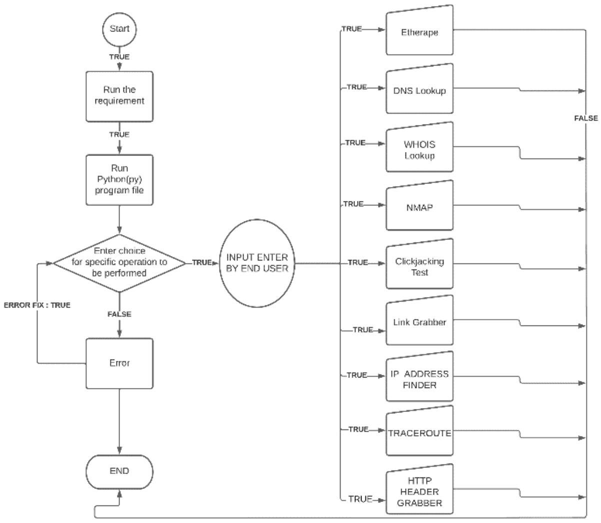


Figure 2 Data flow diagram of proposed system

DFD graphically representing the functions, or processes, which capture, manipulate, store, and distribute data between a system and its environment and between components of a system. The visual representation makes it a good communication tool between User and System designer. Structure of DFD allows starting from a broad overview and expand it to a hierarchy of detailed diagrams. DFD has often been used due to the following reasons:

- Logical information flow of the system
- Determination of physical system construction requirements
- Simplicity of notation
- Establishment of manual and automated systems requirements.

Etherape

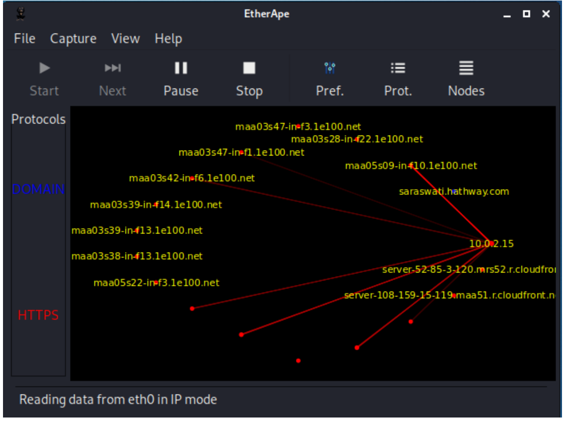
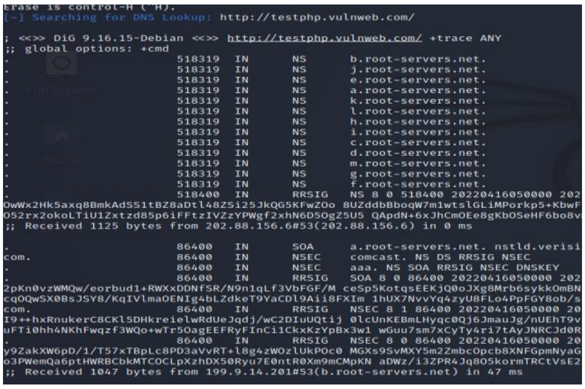

EtherApe
File
Capture
View
Help
Start
Next
Pause
Stop
Pref.
Prot.
Nodes
Protocols
DOMAIN
HTTPS
maa03s47-in-f3.1e100.net
maa03s28-in-f22.1e100.net
maa03s47-in-f1.1e100.net
maa05s09-in-f10.1e100.net
maa03s42-in-f6.1e100.net
saraswati.hathway.com
maa03s39-in-f14.1e100.net
maa03s39-in-f13.1e100.net
10.0.2.15
maa03s38-in-f13.1e100.net
server-52-85-3-120.mrs52.r.cloudfro
maa05s22-in-f3.1e100.net
server-108-159-15-119.maa51.r.cloudfront.n
Reading data from eth0 in IP mode

Fig 3 The diagram shows the live traffic between the enduser and Internet.

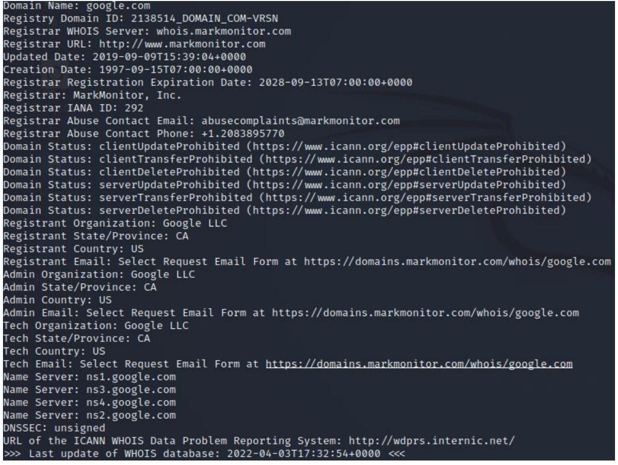
DNS Loook up



```
Erase is control-H (^H).
[-] Searching for DNS Lookup: http://testphp.vulnweb.com/

; <<>> DiG 9.16.15-Debian <<>> http://testphp.vulnweb.com/ +trace ANY
;; global options: +cmd
.                       518319  IN      NS      b.root-servers.net.
.                       518319  IN      NS      j.root-servers.net.
.                       518319  IN      NS      e.root-servers.net.
.                       518319  IN      NS      a.root-servers.net.
.                       518319  IN      NS      k.root-servers.net.
.                       518319  IN      NS      l.root-servers.net.
.                       518319  IN      NS      h.root-servers.net.
.                       518319  IN      NS      i.root-servers.net.
.                       518319  IN      NS      c.root-servers.net.
.                       518319  IN      NS      d.root-servers.net.
.                       518319  IN      NS      m.root-servers.net.
.                       518319  IN      NS      g.root-servers.net.
.                       518319  IN      NS      f.root-servers.net.
.                       518400  IN      RRSIG   NS 8 0 518400 20220416050000 202
OwWx2Hk5axq8BmkAdSS1tBZ8aDtl48ZSi25JkQG5KFwZOo 8UZddbBboqW7m1wtslGLiMPorkp5+KbwF
O52rx2okoLTiU1Zxtzd85p6iFFtzIVZzYPWgf2xhN6D5OgZ5U5 QApdN+6xJhCmOEe8gKbOSeHF6bo8v
;; Received 1125 bytes from 202.88.156.6#53(202.88.156.6) in 0 ms

.                       86400   IN      SOA     a.root-servers.net. nstld.verisi
com.                    86400   IN      NSEC    comcast. NS DS RRSIG NSEC
.                       86400   IN      NSEC    aaa. NS SOA RRSIG NSEC DNSKEY
.                       86400   IN      RRSIG   SOA 8 0 86400 20220416050000 202
2pKn0vzWMQw/eorbud1+RWXxDDNfSR/N9n1qLf3VbFGF/M ceSp5KotqsEEKjQ0oJXg8Mrb6sykkOmBN
cqOQwSX0BsJSY8/KqIVlmaOENIg4bLZdkeT9YaCDl9Aii8FXIm 1hUX7NvvYq4zyU8FLo4PpFGY8ob/s
com.                    86400   IN      RRSIG   NSEC 8 1 86400 20220416050000 20
I9++hxRnukerC8CKl5DHkreielwRdUeJqdj/wC2DIuUQtij 0lcUnKEBmLHyqc0Qj6JmauJg/nUEhT9v
uFTi0hh4NKhFwqzf3WQo+wTr5OagEEFRyFInCi1CkxKzYpBx3w1 wGuu7sm7xCyTy4ri7tAyJNRCJd0R
.                       86400   IN      RRSIG   NSEC 8 0 86400 20220416050000 20
y9ZakXW6pD/1/T57xTBpLc8PD3aVvRT+l8g4zWOzlUkPOc0 MGXs9SvMXY5m2ZmbcOpcb8XNFGpmNyaG
o3PWemQa6ptHWRBCbkMTCOCLpXzhDX50Ryu7E0ntR0Xm9mCMpKN aDWz/i3ZPR4Jq8O5kormTRCtVsE2
;; Received 1047 bytes from 199.9.14.201#53(b.root-servers.net) in 47 ms
```

Fig 4 Subdomain and information of testphp.vulnweb.com.

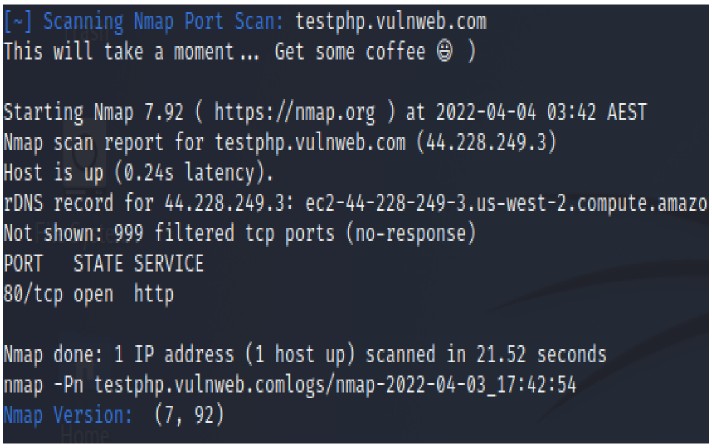
Who is loopk up



```
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: 2019-09-09T15:39:04+0000
Creation Date: 1997-09-15T07:00:00+0000
Registrar Registration Expiration Date: 2028-09-13T07:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registrant Organization: Google LLC
Registrant State/Province: CA
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Admin Organization: Google LLC
Admin State/Province: CA
Admin Country: US
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Tech Organization: Google LLC
Tech State/Province: CA
Tech Country: US
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/google.com
Name Server: ns1.google.com
Name Server: ns3.google.com
Name Server: ns4.google.com
Name Server: ns2.google.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2022-04-03T17:32:54+0000 <<<
```

Fig 5 Domain information

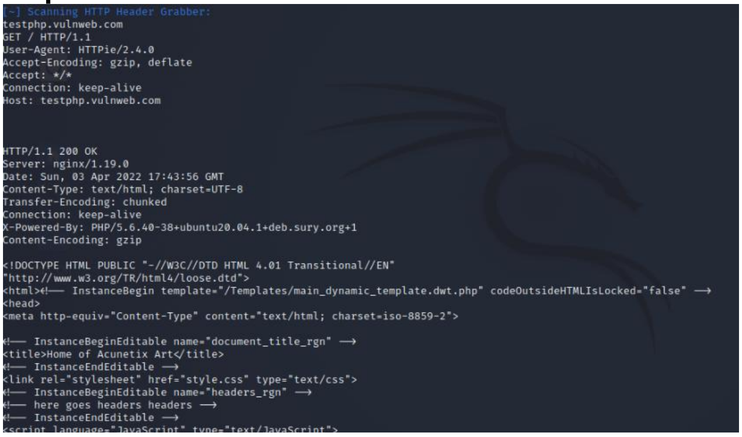
Nmap Port Scan



```
[~] Scanning Nmap Port Scan: testphp.vulnweb.com
This will take a moment... Get some coffee 😋 )

Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-04 03:42 AEST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.24s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazo
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 21.52 seconds
nmap -Pn testphp.vulnweb.comlogs/nmap-2022-04-03_17:42:54
Nmap Version:  (7, 92)
```

Fig 6 It scan ports which are available or open in a domain

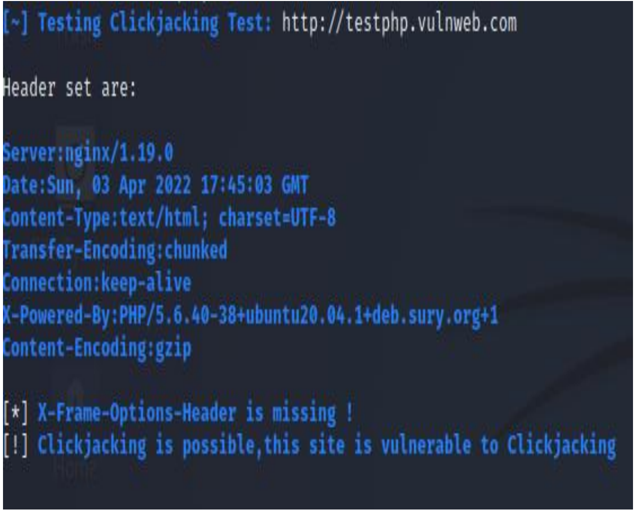
Http Header Grabber.



```
[~] Scanning HTTP Header Grabber:
testphp.vulnweb.com
GET / HTTP/1.1
User-Agent: HTTPie/2.4.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Host: testphp.vulnweb.com



HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Sun, 03 Apr 2022 17:43:56 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!— InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false" —>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!— InstanceBeginEditable name="document_title_rgn" —>
<title>Home of Acunetix Art</title>
<!— InstanceEndEditable —>
<link rel="stylesheet" href="style.css" type="text/css">
<!— InstanceBeginEditable name="headers_rgn" —>
<!— here goes headers headers —>
<!— InstanceEndEditable —>
<script language="JavaScript" type="text/JavaScript">
```

Fig 7 Domain connection information and html tags

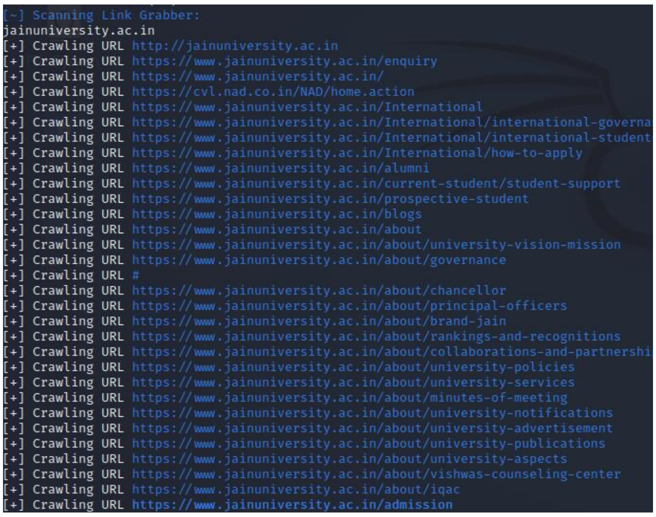
Click jacking



```
[~] Testing Clickjacking Test: http://testphp.vulnweb.com

Header set are:

Server:nginx/1.19.0
Date:Sun, 03 Apr 2022 17:45:03 GMT
Content-Type:text/html; charset=UTF-8
Transfer-Encoding:chunked
Connection:keep-alive
X-Powered-By:PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding:gzip

[*] X-Frame-Options-Header is missing !
[!] Clickjacking is possible,this site is vulnerable to Clickjacking
```

Fig 7 It checks the domain if clickjacking vulnerability is present or not.

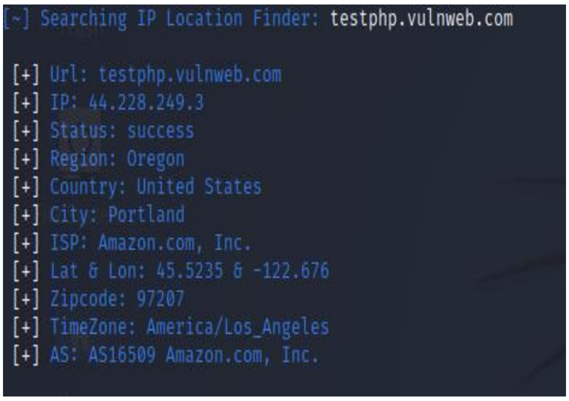
Link Grabber



```
[~] Scanning Link Grabber:
jainuniversity.ac.in
[+] Crawling URL http://jainuniversity.ac.in
[+] Crawling URL https://www.jainuniversity.ac.in/enquiry
[+] Crawling URL https://www.jainuniversity.ac.in/
[+] Crawling URL https://cvl.nad.co.in/NAD/home.action
[+] Crawling URL https://www.jainuniversity.ac.in/International
[+] Crawling URL https://www.jainuniversity.ac.in/International/international-governa
[+] Crawling URL https://www.jainuniversity.ac.in/International/international-student
[+] Crawling URL https://www.jainuniversity.ac.in/International/how-to-apply
[+] Crawling URL https://www.jainuniversity.ac.in/alumni
[+] Crawling URL https://www.jainuniversity.ac.in/current-student/student-support
[+] Crawling URL https://www.jainuniversity.ac.in/prospective-student
[+] Crawling URL https://www.jainuniversity.ac.in/blogs
[+] Crawling URL https://www.jainuniversity.ac.in/about
[+] Crawling URL https://www.jainuniversity.ac.in/about/university-vision-mission
[+] Crawling URL https://www.jainuniversity.ac.in/about/governance
[+] Crawling URL #
[+] Crawling URL https://www.jainuniversity.ac.in/about/chancellor
[+] Crawling URL https://www.jainuniversity.ac.in/about/principal-officers
[+] Crawling URL https://www.jainuniversity.ac.in/about/brand-jain
[+] Crawling URL https://www.jainuniversity.ac.in/about/rankings-and-recognitions
[+] Crawling URL https://www.jainuniversity.ac.in/about/collaborations-and-partnershi
[+] Crawling URL https://www.jainuniversity.ac.in/about/university-policies
[+] Crawling URL https://www.jainuniversity.ac.in/about/university-services
[+] Crawling URL https://www.jainuniversity.ac.in/about/minutes-of-meeting
[+] Crawling URL https://www.jainuniversity.ac.in/about/university-notifications
[+] Crawling URL https://www.jainuniversity.ac.in/about/university-advertisement
[+] Crawling URL https://www.jainuniversity.ac.in/about/university-publications
[+] Crawling URL https://www.jainuniversity.ac.in/about/university-aspects
[+] Crawling URL https://www.jainuniversity.ac.in/about/vishwas-counseling-center
[+] Crawling URL https://www.jainuniversity.ac.in/about/iqac
[+] Crawling URL https://www.jainuniversity.ac.in/admission
```

Fig 8: Possible domains associated with the main domain.

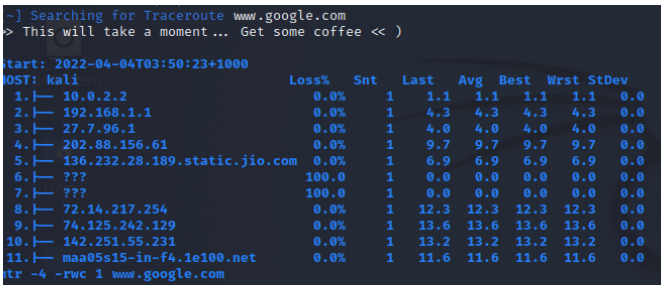
Ip Location Finder.



```
[~] Searching IP Location Finder: testphp.vulnweb.com

 [+] Url: testphp.vulnweb.com
 [+] IP: 44.228.249.3
 [+] Status: success
 [+] Region: Oregon
 [+] Country: United States
 [+] City: Portland
 [+] ISP: Amazon.com, Inc.
 [+] Lat & Lon: 45.5235 & -122.676
 [+] Zipcode: 97207
 [+] TimeZone: America/Los_Angeles
 [+] AS: AS16509 Amazon.com, Inc.
```

Fig 9: The IP location of domain server.

Traceroute



```
~] Searching for Traceroute www.google.com
> This will take a moment ... Get some coffee << )

tart: 2022-04-04T03:50:23+1000
OST: kali                              Loss%   Snt   Last   Avg  Best  Wrst StDev
 1.|-- 10.0.2.2                         0.0%     1    1.1   1.1   1.1   1.1   0.0
 2.|-- 192.168.1.1                      0.0%     1    4.3   4.3   4.3   4.3   0.0
 3.|-- 27.7.96.1                        0.0%     1    4.0   4.0   4.0   4.0   0.0
 4.|-- 202.88.156.61                    0.0%     1    9.7   9.7   9.7   9.7   0.0
 5.|-- 136.232.28.189.static.jio.com    0.0%     1    6.9   6.9   6.9   6.9   0.0
 6.|-- ???                             100.0     1    0.0   0.0   0.0   0.0   0.0
 7.|-- ???                             100.0     1    0.0   0.0   0.0   0.0   0.0
 8.|-- 72.14.217.254                    0.0%     1   12.3  12.3  12.3  12.3   0.0
 9.|-- 74.125.242.129                   0.0%     1   13.6  13.6  13.6  13.6   0.0
10.|-- 142.251.55.231                   0.0%     1   13.2  13.2  13.2  13.2   0.0
11.|-- maa05s15-in-f4.1e100.net         0.0%     1   11.6  11.6  11.6  11.6   0.0
tr -4 -rwc 1 www.google.com
```

Fig 10: Displays the intermediate node for router to reach google.com in limited time.

The above information about several domain is crucial and how it's easy to get hand on it because of the evolution pf technologies. Information gathering plays a huge role on the success of hacking domain ethically or unethically. The information which was gathered during the reconnaissance can led to various attack and led to financial loss and reputation damage. Normal user is unaware of the tool which are used by the hacker to gathered information in short period of time.

As the technology upgrade its very necessary to know about the tools and safeguard policy in order to preempt several attacks. Data is like a new oil, which is going to play vital role in human life in upcoming ten years. It's the responsibility of cyber professional to comprise the data collections using different types of open source of tool for information gathering by invoking the necessary protocol and policy. The above figures are just a proper example of how unethical hacker can fetch data and manipulated end-user mentality and behavior and cause severe effect of respective domain which ultimate effect the user of the specific domain. So, it's important to fix the loopholes and enabled respective policy and controls which minimize the information gathering without end-user consent.

VI.CONCLUSION

The Proposed system works well open source tool arranged into one place or environment. The proposed system is effective against workloads and provides simplicity. Reconnaissance is a primary and beginning segment of any cyber-attack so if any solution for detecting cyber reconnaissance may be an excellent fulfilment in the direction of improvement on powerful early warning system. It is necessary to understand about the intentions, mentality and working of hacker, ethical hacker and cybersecurity tools which is very crucial in order to protect the data available in public domains. The benefits of better knowledge about cybersecurity tools can identify and prevents lot of attacks surfacing applications and as well as web applications or anything which have IP address. Reconnaissance is an essential first phase of cybersecurity which speed up the process of information gathering against the target or hacker using open source tools. Since the technology's advancement, day by day lots of vulnerabilities are been discovered surfacing over application software and web application.

It is an early warning to all the cyber security professional, researcher and students throughout the worldwide to work hard in finding the effective solutions for upcoming threats and existing threats.Security is a 24/7 job. If a person is concerned for his security, he or she needs to take care of it constantly. Even the information gathering is not a solution for our security, the system needs to upgraded and enhanced constantly. People should be educated regarding the security of their data and information and how much important it is in this internet era.

The proposed system also needs enhancement and it needs to be upgraded. So, that it can even perform its functions more properly. In the next version of the proposed system traceroute,crawler,link grabber and ip location finder. No system is complete, the proposed system also has some shortcomings which will be addressed in the future. The proposed system will have more specific operation like detecting vulnerability HTML injection, Open Redirect and traceroute will be add in the future enhancement.

REFERENCES

[1] Wojciech Mazurczak, Luca Caviglione, Cyber Reconnaissance Techniques, Communications of the ACM, Vol. 64 No. 3, Pages 86-95 10.1145/3418293, March 2021

[2] Shanto Roy, Nazia Sharmin, Jamie C. Acosta, Christopher Kiekintveld, Aron Laszka, Survey and Taxonomy of Adversarial Reconnaissance Technique, arXiv:2105.04749v1 [cs.CR], May 2021,

[3] Danda B. Rawat, Journal on Cybersecurity and Privacy, Journal of Cybersecurity and Privacy: A New Open Access Journal, 2021

[4] Abdulkadir Bilen and Ahmet Bedri Azur , Cyber-attack method and perpetrator prediction using machine learning algorithms, s. PeerJ Comput. Sci. 7: e475 DOI 10.7717/peerj-cs.475, 2021

[5] Ahmad Mtair AL Hawamleh, Alorfi Almuhannad Sulaiman M, Jassim Ahmad Al-Gasawneh, Ghada Al-Rawashdeh , Cyber Security and Ethical Hacking: The Importance of Protecting User Data Solid State Technology, Volume: 63 Issue: 5, 2020

[6] Rohit Kalakuntla, Anvesh Babu Vanamala, Ranjith Reddy Kolipyaka , Cyber Security, 2019, HOLISTICA Vol 10, Issue 2, pp. 115-128, 2019

[7] Idimadakala Nagaraju, Ethics in Ethical Hacking, International Journal of Scientific & Engineering Research, Volume 4, Issue 10,ISSN 2229-5518, 2018

[8] Saloni Khurana, A Review Paper on Cyber Security International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Published by, www.ijert.org, VIMPACT - 2017 Conference Proceedings, 2017

[9] Pavan Kumar, K. Pranathi, A Survey on Ethical Hacking, Approaches, Attacks, Procedure & Reliability in case of Cyber Crime. JAC: A Journal of Composition Theory Volume XIV, Issue IV, APRIL 2021 ISSN: 0731-6755,2017

[10] Brijesh Kumar Pandey, Alok Singh and Lovely lakhmani Balani, ETHICAL HACKING (Tools, Techniques and Approaches, Conference Paper · January 2017(CAIM-International Conference on Advancement in IT and Management At: Thakur Institute of Management Studies Career Development and Research Thakur Village Kandivali East Mumbai),2017

[11] Victor-Valeriu Patriciu and Adrian Constantin Furtuna, Guide for Designing Cyber Security Exercises recent advances in e-activities, information security and privacy (ISSN: 1790-5117 ISBN: 978-960-474-143-4), 2016

[12] Vikki Davies, Cyber security, The History of Cyber security, https://cybermagazine.com/cyber-security/history-cybersecurity, Oct 2021;

[13]https://owasp.org/www-project-top-ten/: Vulnerabilities in web applications

[14] Workshops, certification and training on cyber security

https://www.eccouncil.org/ethical-hacking/ : Ethical Hacking learnings

Author's details

Manoj Saha[1], Vijayakumar Adaickalam
1: Final Year PG Student, School of Computer Science and Information Technology, Jain Deemed-to-be University, Bengaluru, India
2: Professor, School of Computer Science and Information Technology, Jain Deemed-to-be University, Bengaluru, India
Email:sahamanoj96@gmail.com[1],
vijay.pattukkottai@gmail.com[2]