

GhostEye



GhostEye is an information gathering, footprinting, scanner, and Reconnaissance tool built with Python 3. It captures information about the target and gives us detailed information about our objectives.

Features:

- It is a user-friendly tool.
- Provide an option to select for our attack preference.
- It has a feature of **Etherape** which is a **Graphical Network Monitor** and a **packet sniffer** that collects information and displays it graphically.
- Etherape is compatible with **Ethernet, FDDI, Token Ring, ISDN, PPP, SLIP, and WLAN devices**, as well as a variety of encapsulations.
- It can filter traffic to be shown and read packets from files as well as actual network data.

Installation:

- **Step 1:**

Install Python3 on Kali using the following command:

sudo apt install python3

```

(kali㉿kali)-[~/Ghost_Eye]
$ sudo apt install python3
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
python3 is already the newest version (3.9.2-1kali1).
The following packages were automatically installed and are no longer required:
  python-babel-localedata python3-babel
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

```

- **Step 2:**

In addition, you need to install the Nmap and EtherApe tools using the following command:

sudo apt install nmap etherape

```

(kali㉿kali)-[~/Ghost_Eye]
$ sudo apt install nmap etherape
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
nmap is already the newest version (7.91+dfsg1-1kali1).
The following packages were automatically installed and are no longer required:
  python-babel-localedata python3-babel
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  etherape-data libgoocanvas-2.0-9 libgoocanvas-2.0-common
The following NEW packages will be installed:
  etherape etherape-data libgoocanvas-2.0-9 libgoocanvas-2.0-common
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 1,017 kB of archives.
After this operation, 5,304 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 etherape-data

```

- **Step 3:**

If you have completed the above requirements, then, you can proceed to the next step and clone the Ghost Eye repo using the following command:

[git clone https://github.com/BullsEye0/ghost_eye.git](https://github.com/BullsEye0/ghost_eye.git)

```
(kali㉿kali)-[~/Ghost_Eye]
$ git clone https://github.com/BullsEye0/ghost_eye.git
Cloning into 'ghost_eye' ...
remote: Enumerating objects: 85, done.
remote: Counting objects: 100% (32/32), done.
remote: Compressing objects: 100% (32/32), done.
remote: Total 85 (delta 16), reused 0 (delta 0), pack-reused 53
Receiving objects: 100% (85/85), 1.26 MiB | 2.46 MiB/s, done.
Resolving deltas: 100% (40/40), done.

(kali㉿kali)-[~/Ghost_Eye]
$
```

- **Step 4:**

The tool has been downloaded and cloned successfully. Now to list out the contents of the tool use the following command.

ls

```
(kali㉿kali)-[~/Ghost_Eye]
$ ls
ghost_eye
```

- **Step 5:**

Now that the Github archive file (i.e. ghost_eye) is installed in Kali, we need to change the working directory to the Ghost Eye folder.

cd ghost_eye

```
(kali㉿kali)-[~/Ghost_Eye]
$ cd ghost_eye

(kali㉿kali)-[~/Ghost_Eye/ghost_eye]
```

- **Step 6:**

You are now in the tool's directory. The following command will list the contents of the directory.

ls

```
(kali㉿kali)-[~/Ghost_Eye/ghost_eye]
$ ls
featured-image.png  LICENSE  requirements.txt
ghost_eye.py        README.md

(kali㉿kali)-[~/Ghost_Eye/ghost_eye]
```

- **Step 7:**

All the files in the tool are listed here. You may need to install tool requirements. To install the requirements, run the following command:

pip3 install -r requirements.txt


```

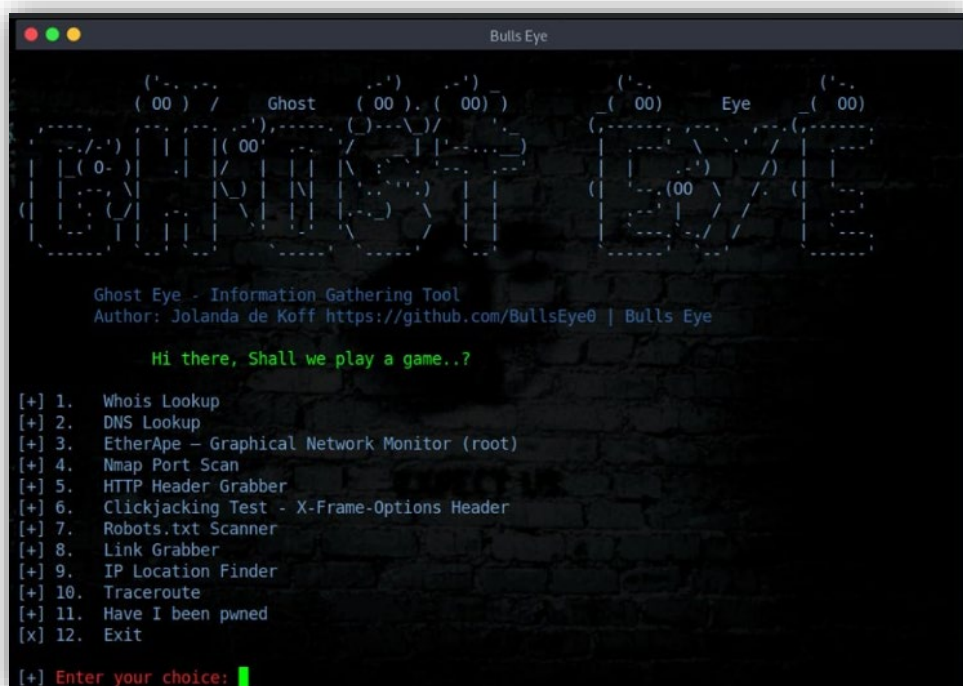
(kali㉿kali)-[~/Ghost_Eye/ghost_eye]
$ pip3 install -r requirements.txt
Requirement already satisfied: beautifulsoup4 in /usr/l
e 1)) (4.9.3)
Collecting cfscrape
  Downloading cfscrape-2.1.1-py3-none-any.whl (12 kB)
Collecting python-nmap
  Downloading python-nmap-0.6.4.tar.gz (43 kB)
  |████████████████████████████████████████| 43 kB 1.0 MB/s
Requirement already satisfied: requests in /usr/lib/pyt
(2.25.1)
Requirement already satisfied: urllib3 in /usr/lib/pyth
1.26.4)
Collecting webtech
  Downloading webtech-1.2.12-py3-none-any.whl (120 kB)
  |████████████████████████████████████████| 120 kB 3.8 MB/s
Requirement already satisfied: soupsieve>1.2 in /usr/li
ements.txt (line 1)) (2.2.1)
Building wheels for collected packages: python-nmap

```

- **Step 8:**

All requirements have been downloaded. Now it's time to start the tool using the following command:

python3 *ghost_eye.py*



```

Bulls Eye

  ('..')
  ( 00 ) /   Ghost   ( 00 ) . ( 00 )
  ('..')
  ( 00 ) Eye   ('..')
  ( 00 )

  Ghost Eye - Information Gathering Tool
  Author: Jolanda de Koff https://github.com/BullsEye0 | Bulls Eye

  Hi there, Shall we play a game..?

[+] 1.  Whois Lookup
[+] 2.  DNS Lookup
[+] 3.  EtherApe - Graphical Network Monitor (root)
[+] 4.  Nmap Port Scan
[+] 5.  HTTP Header Grabber
[+] 6.  Clickjacking Test - X-Frame-Options Header
[+] 7.  Robots.txt Scanner
[+] 8.  Link Grabber
[+] 9.  IP Location Finder
[+] 10. Traceroute
[+] 11. Have I been pwned
[x] 12. Exit

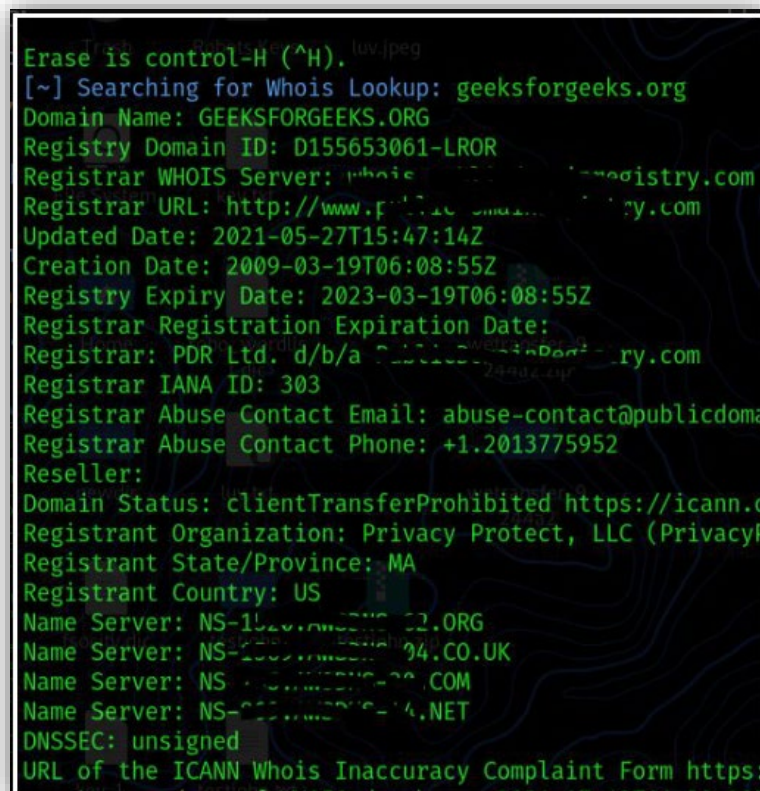
[+] Enter your choice: █

```

Usage:

- **Whols Lookup**

Whols searches the Whois database for an object. Whois a query and response protocol commonly used to access databases that show users from an Internet source, such as a domain name or IP address.



```
Erase is control-H (^H).
[~] Searching for Whois Lookup: geeksforgeeks.org
Domain Name: GEEKSFORGEEKS.ORG
Registry Domain ID: D155653061-LROR
Registrar WHOIS Server: whois.registry.com
Registrar URL: http://www.publicdomainregistry.com
Updated Date: 2021-05-27T15:47:14Z
Creation Date: 2009-03-19T06:08:55Z
Registry Expiry Date: 2023-03-19T06:08:55Z
Registrar Registration Expiration Date:
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp/#clientTransferProhibited
Registrant Organization: Privacy Protect, LLC (Privacy Protected)
Registrant State/Province: MA
Registrant Country: US
Name Server: NS-1528.AWSCNS-02.ORG
Name Server: NS-1529.AWSCNS-04.CO.UK
Name Server: NS-1530.AWSCNS-06.COM
Name Server: NS-1531.AWSCNS-08.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/whois-inaccuracy-complaint-form
```

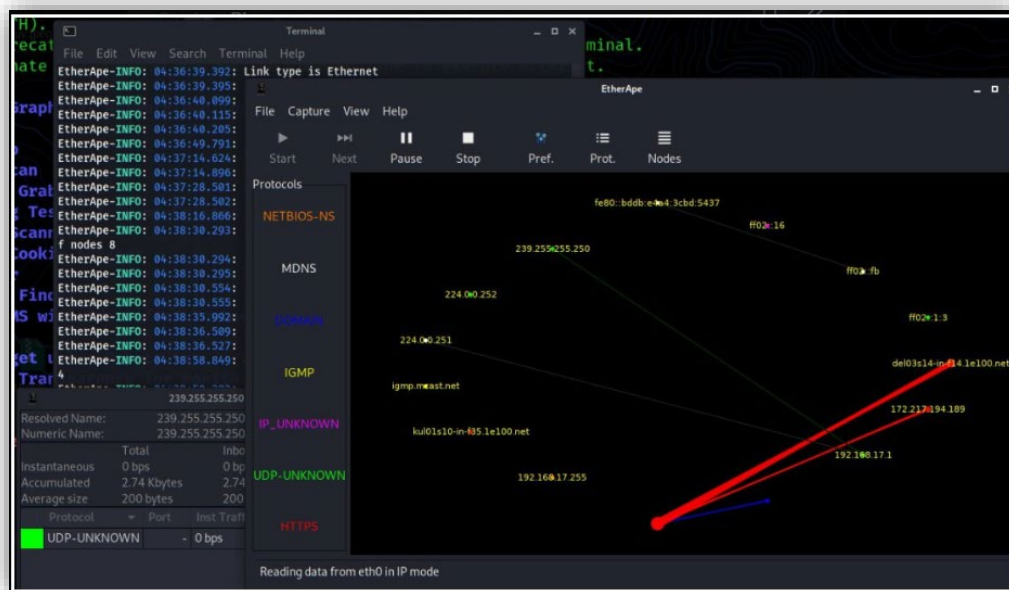
- **DNS Lookup**

The next option that we will discuss is the **DNS Lookup tool** (Option 2 in Ghost Eye tool). DNS stands for "**Domain Name System**" and is the process by which a DNS record has been returned from a DNS server. Just like looking up a phone number in a phone book - that's why it's referred to as a "lookup". Interconnected computers, servers, and smartphones need to know how to

translate the email addresses and domain names people use into meaningful numerical addresses. A DNS lookup performs this function.

- **Etherape – Graphical Network Monitor**

It is a graphical network monitor and packet sniffer that collects and displays information graphically. It can also filter the traffic shown and read packets from a file as well as live from the network.



- **Nmap Port Scan**

Nmap port scan looks for open ports on the provided connection or IP address. In the Ghost Eye script, a nmap **-Pn** scan is utilized. **-pn** causes all hosts to be treated as online, bypassing host discovery.

```
[~] Scanning Nmap Port Scan: geeksforgeeks.org
This will take a moment... Get some coffee ☺ )

Host discovery disabled (-Pn). All addresses will be marked 'up' and
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-17 04:48 EDT
Nmap scan report for geeksforgeeks.org (34.218.62.116)
Host is up (0.28s latency).
rDNS record for 34.218.62.116: ec2-34-218-62-116.us-west-2.compute.a
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 62.39 seconds
nmap -Pn geeksforgeeks.org logs/nmap-2021-07-17 08:49:47
```

- **Clickjacking test**

An attacker uses a transparent iframe in a window to direct the user to click a button or link to take another server with a similar-looking window. In a sense, the attacker captures the clicks intended for the original server and redirects them to the alternate server.

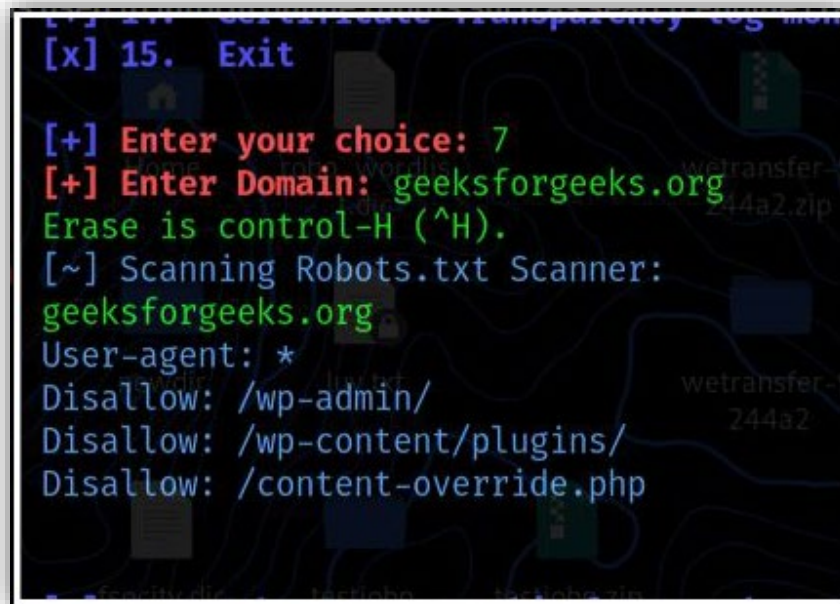
```
[+] Enter your choice: 6
[+] Enter the Domain to test: geeksforgeeks.org
Erase is control-H (^H).
[~] Testing Clickjacking Test: http://geeksforgeeks.org

Header set are:
Server:nginx
Content-Type:text/html; charset=UTF-8
X-Frame-Options:DENY
Content-Encoding:gzip
X-Akamai-Transformed:9 - 0 pmb=mRUM,2
Cache-Control:max-age=21286
Date:Sat, 17 Jul 2021 08:55:34 GMT
Content-Length:19261
Connection:keep-alive
Vary:Accept-Encoding
Server-Timing:cdn-cache; desc=HIT, edge; dur=1

[+] Click Jacking Header is present
[+] You can't clickjack this site !
```


- **Robots.txt Scanner**

The robots.txt file is used to inform online robots such as search engine crawlers about which areas of the website robots are allowed to explore and index.



```
[x] 15. Exit  
[+] Enter your choice: 7  
[+] Enter Domain: geeksforgeeks.org  
Erase is control-H (^H).  
[~] Scanning Robots.txt Scanner:  
geeksforgeeks.org  
User-agent: *  
Disallow: /wp-admin/  
Disallow: /wp-content/plugins/  
Disallow: /content-override.php
```

- **Link Grabber**

Link Grabber will analyse the HTML source code of a website and retrieve links from it. For simple review hrefs or pages, links are shown in plain text.

```
[+] Enter your choice: 9
[+] Enter Domain: geeksforgeeks.org

File System  key.txt
Home  robo_jeordius  webtransfer-9
       index        244a2.zip

Erase is control-H (^H).
[~] Scanning Link Grabber:
geeksforgeeks.org
[+] Crawling URL http://geeksforgeeks.org
[+] Crawling URL #main
[+] Crawling URL https://www.geeksforgeeks.org/
[+] Crawling URL https://www.geeksforgeeks.org/analysis-of-algori
[+] Crawling URL https://www.geeksforgeeks.org/analysis-of-algori
[+] Crawling URL https://www.geeksforgeeks.org/analysis-of-algori
[+] Crawling URL https://www.geeksforgeeks.org/analysis-of-algori
[+] Crawling URL https://www.geeksforgeeks.org/lower-and-upper-bo
[+] Crawling URL https://www.geeksforgeeks.org/analysis-of-algori
[+] Crawling URL https://www.geeksforgeeks.org/analysis-algorithm
[+] Crawling URL https://www.geeksforgeeks.org/analysis-algorithm
[+] Crawling URL https://www.geeksforgeeks.org/g-fact-86/?ref=ghm
[+] Crawling URL https://www.geeksforgeeks.org/pseudo-polynomial-
[+] Crawling URL https://www.geeksforgeeks.org/polynomial-time-ap
[+] Crawling URL https://www.geeksforgeeks.org/a-time-complexity-
[+] Crawling URL https://www.geeksforgeeks.org/searching-algorith
[+] Crawling URL https://www.geeksforgeeks.org/sorting-algorithms
[+] Crawling URL https://www.geeksforgeeks.org/graph-data-structu
[+] Crawling URL https://www.geeksforgeeks.org/algorithms-gg/patt
[+] Crawling URL https://www.geeksforgeeks.org/geometric-algorith
[+] Crawling URL https://www.geeksforgeeks.org/mathematical-algor
```

- **IP Location Finder**

We can use the IP Location Finder to find information about a certain URL or IP address. This tool will retrieve the latitude and longitude of the device or server.

```
Teach  Robert_Kay  liv.jpeg
[+] Enter your choice: 10
[+] Enter Domain or IP Address: geeksforgeeks.org
Erase is control-H (^H).
[~] Searching IP Location Finder: geeksforgeeks.org

File System  key.txt
Home  robo_jeordius  webtransfer-9
       index        244a2.zip

[+] Url: geeksforgeeks.org
[+] IP: 34.218.31.110
[+] Status: success
[+] Region: Oregon
[+] Country: United States
[+] City: Portland
[+] ISP: Amazon.com, Inc.
[+] Lat & Lon: 45.5205 3 -122.676
[+] Zipcode: 97207
[+] TimeZone: America/Los_Angeles
[+] AS: AS16509 Amazon.com, Inc.
```

- Crawler Target URL + Robots.txt

```

https://www.geeksforgeeks.org/data-structures
https://www.geeksforgeeks.org/category/progra
https://www.geeksforgeeks.org/articles-on-com
https://www.youtube.com/geeksforgeeksvideos/>
https://practice.geeksforgeeks.org/courses/>C
https://practice.geeksforgeeks.org/company-ta
https://practice.geeksforgeeks.org/topic-tags
https://practice.geeksforgeeks.org/faq.php>Ho
https://www.geeksforgeeks.org/contribute/>Wri
https://www.geeksforgeeks.org/write-interview
https://www.geeksforgeeks.org/careers/?job_ty
https://www.geeksforgeeks.org/how-to-contribu
https://www.geeksforgeeks.org/
https://www.geeksforgeeks.org/copyright-infor
https://www.geeksforgeeks.org/wp-includes/js/
https://www.geeksforgeeks.org/cookie-policy/
https://www.geeksforgeeks.org/privacy-policy/
https://ssl'
http://www')

[+] Robots.txt:
User-agent: *
Disallow: /wp-admin/
Disallow: /wp-content/plugins/
Disallow: /content-override.php

```

- Exit

```

[+] 12. Traceroute
[+] 13. Crawler target url + Robots.txt
[+] 14. Certificate Transparency log monitor
[x] 15. Exit

[+] Enter your choice: 15

Blue Eye DONE... Exiting... Like to See Ya Hacking Anywhere ..!

(kali@kali)~$ cd ~/Ghost_Eve/ghost_eve

```

Advantages of using GhostEye include:

- *Automation of **reconnaissance processes**, which saves time and effort for the user.*
- *Ability to gather a large amount of information about a target in a **short amount of time**.*
- *Integration with other tools for further analysis and exploitation.*
- ***User-friendly interface**, making it easy for both experienced and novice users to utilize.*
- ***Open-source availability**, making it free to use and customize.*
- *It can be used to gather information from various sources like **domain, IP, Email, Website, and Social-Media**.*
- *It can also be used to **check the target's online presence** and **identify any vulnerabilities**.*
- *Can help to **create a comprehensive report of the target's infrastructure**, which can be used to plan and execute a targeted attack.*

REFERENCE

https://www.geeksforgeeks.org/how-to-install-ghost_eye-tool-in-kali-linux/

<https://hackingpassion.com/getting-started-with-ghost-eye/>

<https://hackingpassion.com/ghost-eye-informationgathering-footprinting-and-reconnaissance-tool-release/>