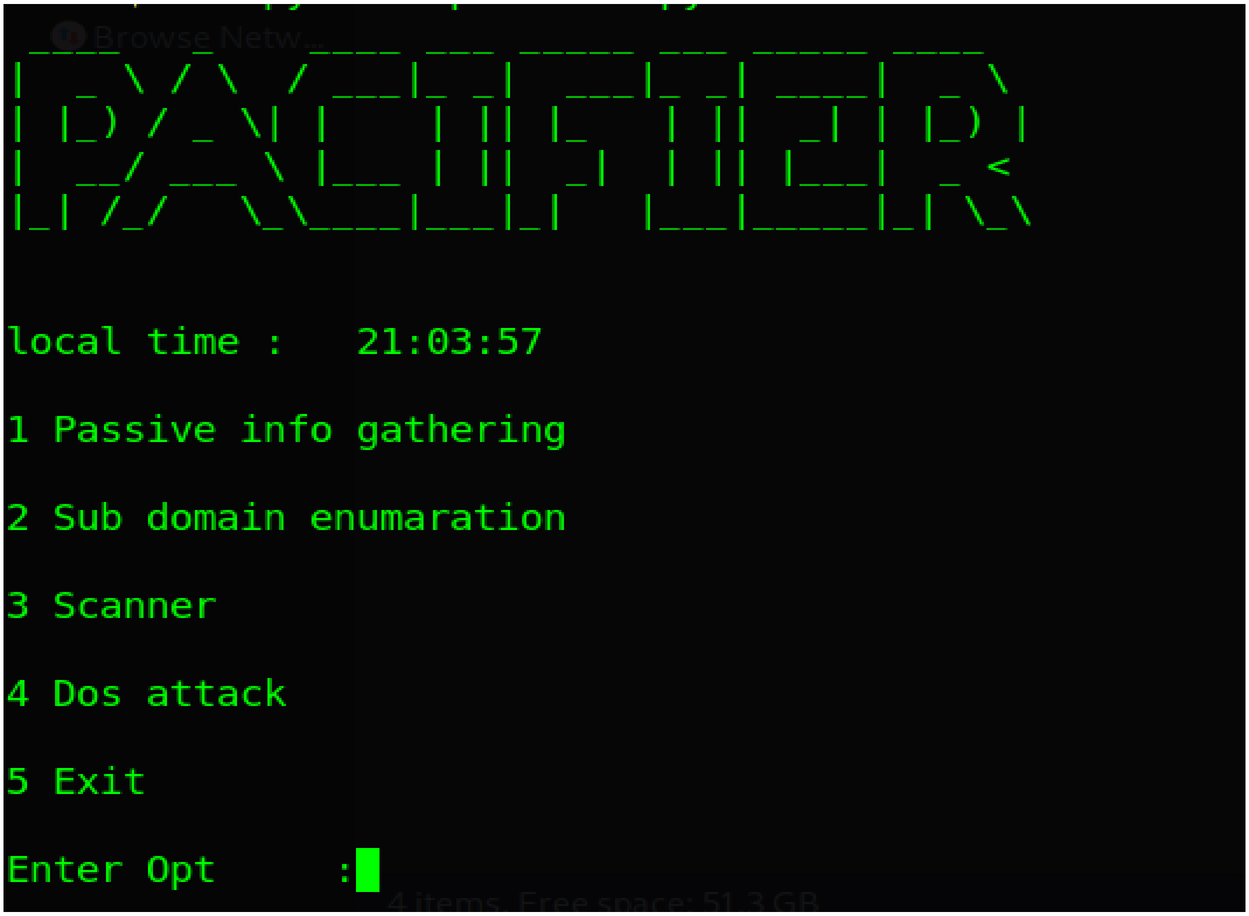
ADCD 07.00 PM Batch 2021

Pacifier.py

Project Documentation (technical)

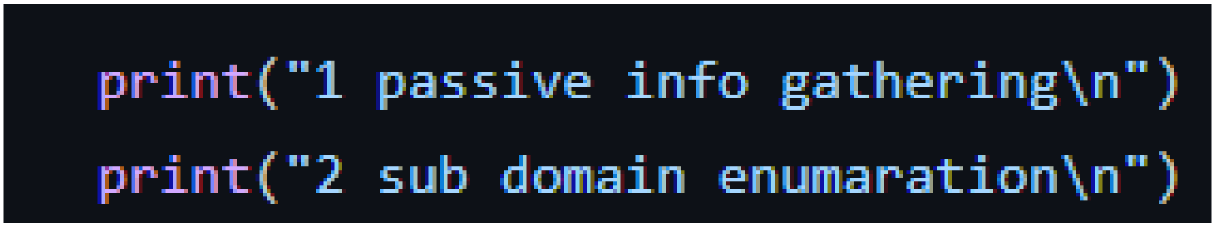


```
 ____   _    ____ ___ _____ ___ _____ ____
|  _ \ / \  / ___|_ _|  ___|_ _| ____|  _ \
| |_) / _ \| |    | || |_   | ||  _| | |_) |
|  __/ ___ \ |___ | ||  _|  | || |___|  _ <
|_| /_/   \_\____|___|_|   |___|_____|_| \_\


local time :   21:03:57

1 Passive info gathering

2 Sub domain enumaration

3 Scanner

4 Dos attack

5 Exit

Enter Opt      :
```

Introduction

PACIFIER is a hundred percent python based program which can be used to do information gathering and ip scanning and a simple Dos attack .

The section Info gathering includes passive info gathering , mostly with google search results and Sub domain enumeration.

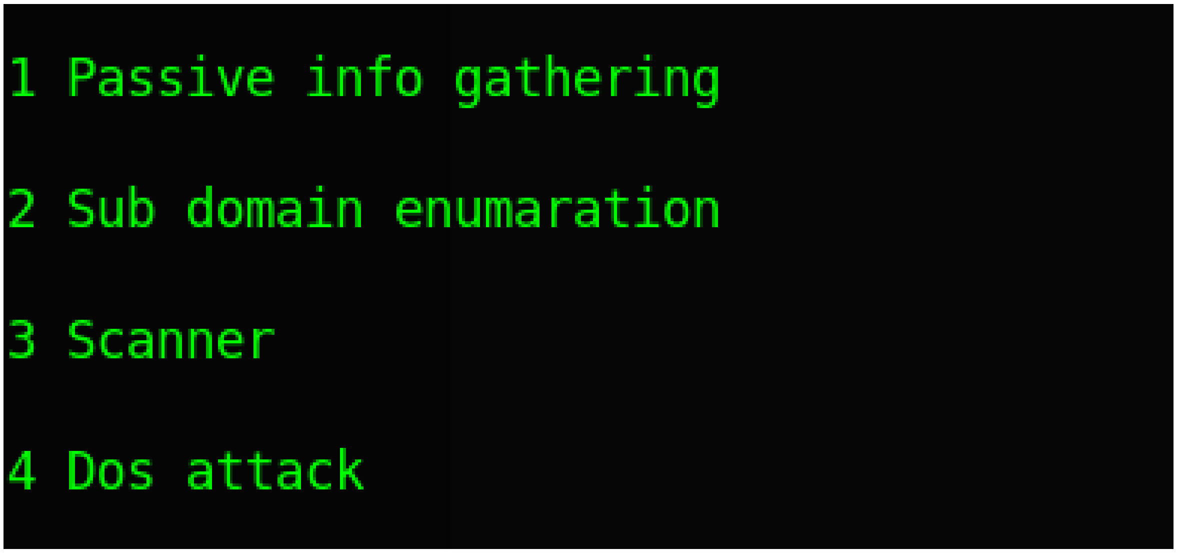


```
print("1 passive info gathering\n")
print("2 sub domain enumaration\n")
```

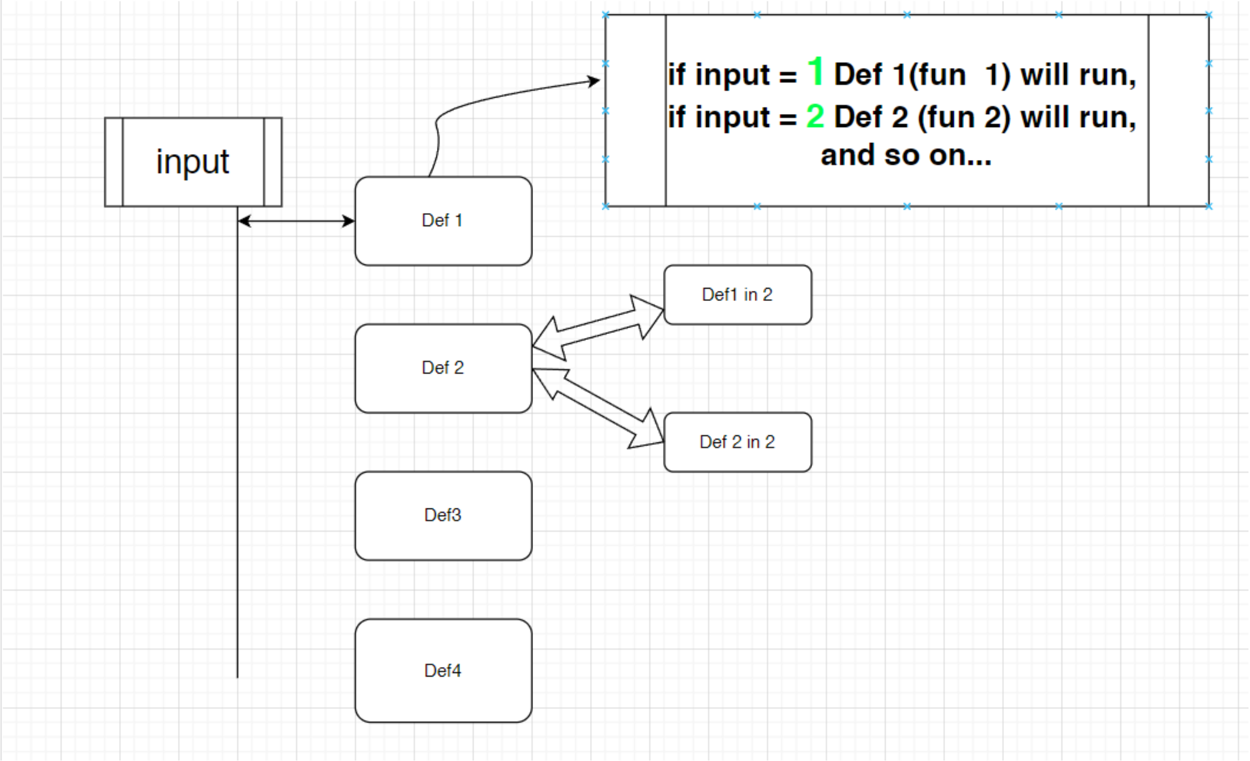
Scanning section includes udp and port scan and for addition we included a Dos attack function too.

Method Of Working

The whole script runs in simple Def keyword along with “ if ” and “ elif ” statements. We packed the basic functions inside four different “ Def “ keywords.



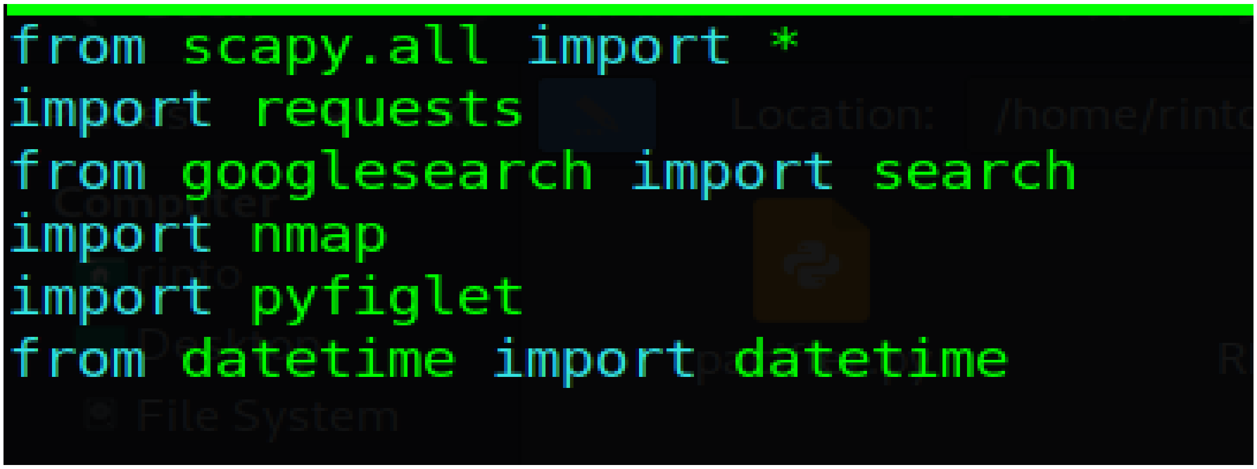
```
1 Passive info gathering

2 Sub domain enumaration

3 Scanner

4 Dos attack
```



if input = 1 Def 1(fun 1) will run,
if input = 2 Def 2 (fun 2) will run,
and so on...

Modules

We used set of modules for making every function in this program,



```
from scapy.all import *
import requests
from googlesearch import search
import nmap
import pyfiglet
from datetime import datetime
```

import Scrapy

Scrapy is a fast high-level web crawling and web scraping framework, used to crawl websites and extract structured data from their pages. It can be used for a wide range of purposes, from data mining to monitoring and automated testing. We used scrapy module to sent fake packets to an ip. That which enable to perform Dos attack function in our project.

Import requests

requests library is the de facto standard for making HTTP requests in Python. It abstracts the complexities of making requests behind a beautiful, simple API so that it can focus on interacting with services and consuming data in your application. It's very important because its enables subdomain enumeration.

Import google

We installed google search module for passive info gathering. in simple terms , it returns Google’s search results.

Import nmap

python-nmap is a python library which helps in using nmap port scanner. It allows to easilly manipulate nmap scan results and will be a perfect tool for systems administrators who want to automatize scanning task and reports. It also supports nmap script outputs. In our program we included two types of scanners , UDP scanner and Port scanner. Its only works if nmap module is installed.

Import pyfiglet

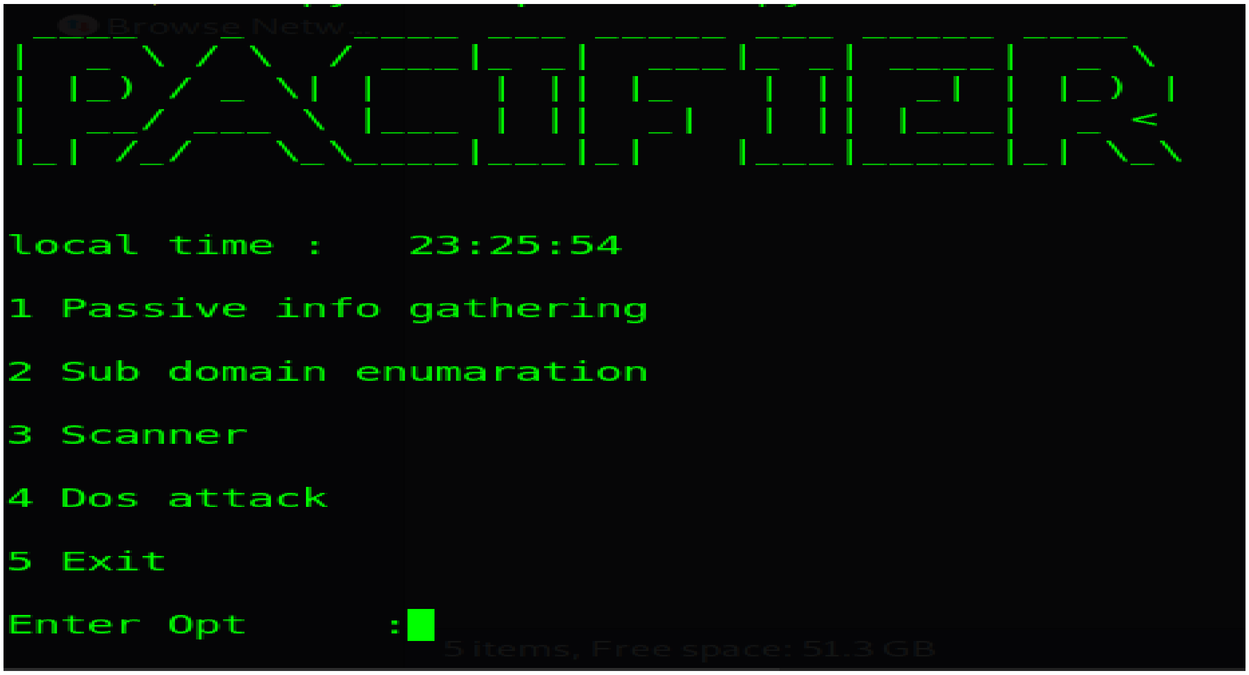
The Pyfiglet module is a Python module that comes with many functions, and we can use these functions in a Python program to create fancy texts with large fonts & sizes in the output. The Pyfiglet module is specially designed to enhance our programming experience as well as to enhance the overall look and structure of the texts used in electronic communication.so its kinda important to our project , just for the look.

Import datetime

In Python, date and time are not a data type of their own, but a module named datetime can be imported to work with the date as well as time. Python Datetime module supplies classes to work with date and time. These classes provide a number of functions to deal with dates, times and time intervals.we are not in to dig in that , we are use this module to print current time.

How it’s work

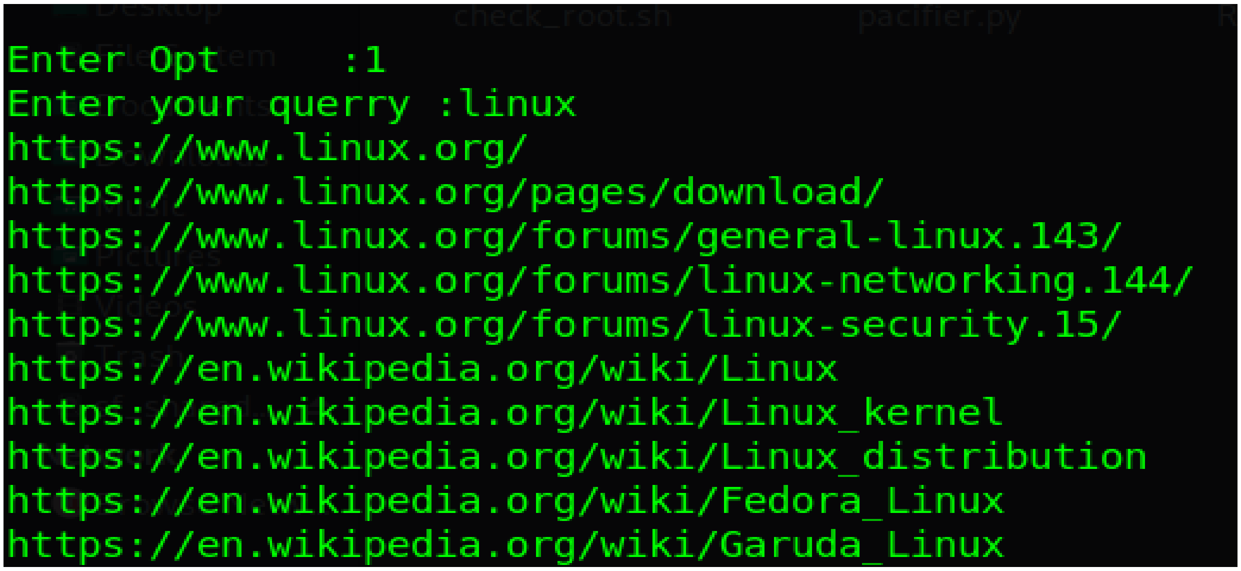
Run PACIFIER.py with root privileges …



```
local time :    23:25:54

1 Passive info gathering

2 Sub domain enumaration

3 Scanner

4 Dos attack

5 Exit

Enter Opt       :
```

And input the option (int) for specified function

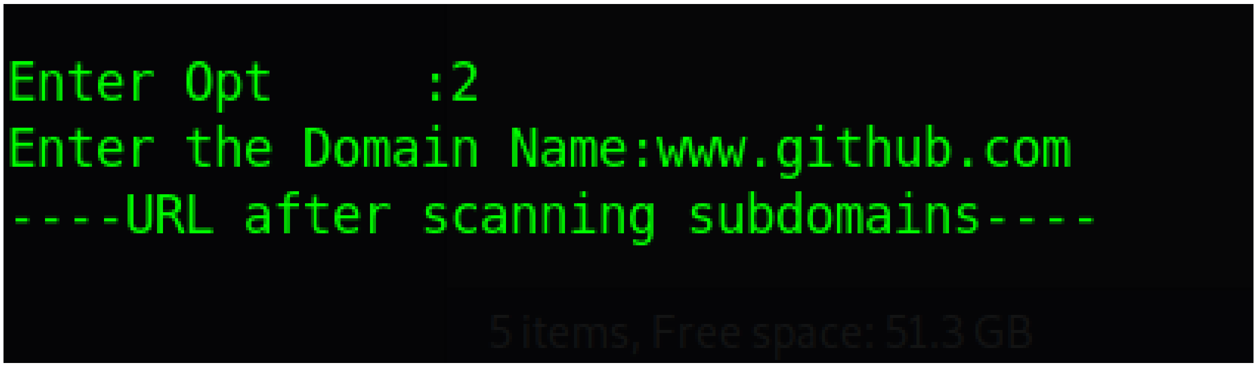
1 passive info gathering



```
Enter Opt     :1
Enter your querry :linux
https://www.linux.org/
https://www.linux.org/pages/download/
https://www.linux.org/forums/general-linux.143/
https://www.linux.org/forums/linux-networking.144/
https://www.linux.org/forums/linux-security.15/
https://en.wikipedia.org/wiki/Linux
https://en.wikipedia.org/wiki/Linux_kernel
https://en.wikipedia.org/wiki/Linux_distribution
https://en.wikipedia.org/wiki/Fedora_Linux
https://en.wikipedia.org/wiki/Garuda_Linux
```

After you select 1 and input your query , pacifier will return top ten google search results of your query.

2 sub domain enumeration



```
Enter Opt     :2
Enter the Domain Name:www.github.com
----URL after scanning subdomains----
```

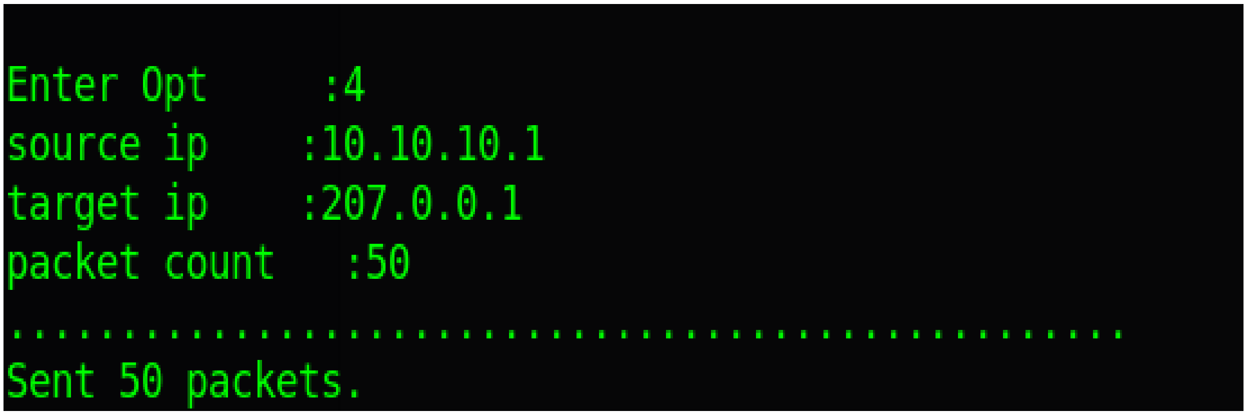
After selecting option 2 enter a Domain , and this tool will return all possible subdomains. *

3 Scanner

You get two options for scanner function. UDP and port scanner , enter the port range (eg:85 to 90) followed by ip number for port scanner and it will show opened and closed ports by given range.

Enter the ip range or ip after selecting udp scan for performing an UDP scan

4 Dos Attack



```
Enter Opt      :4
source ip     :10.10.10.1
target ip     :207.0.0.1
packet count    :50
..................................................
Sent 50 packets.
```

Enter source ip , mosty just a fake ip for showing in interface , next enter the target ip* (which you want to send Dos Attack) and finally, enter number of fake packets you wish to send. the number of packets will determine dept of your attack.

—-----End Of Document—-----

External links we refer;

www.google.com

www.w3schools.com

www.github.com