A PROJECT REPORT

ON

"ANALYSIS AND EXTRACTION OF CRITICAL INFORMATION FROM NETWORK"

Submitted to

VELLORE INSTITUTE OF TECHNOLOGY

BY

MEERAJ GAWDE	**18BCY10120**
GAURAV KACHARE	**18BCY10035**
AKSHAT NIGAM	**18BCY100**
VISHWAJEET MISHRA	**18BCY10116**

UNDER THE GUIDANCE OF
Dr. AJIT KUMAR

DEPARTMENT OF COMPUTER SCIENCE ENGINEERING

VIT BHOPAL UNIVERSITY

LOCATED IN KOTHRI, SEHORE - 466114

2019-2020

AFFILIATED TO

VELLORE INSTITUTE OF TECHNOLOGY

Acknowledgements

We are profoundly grateful to **Dr. AJIT KUMAR** for his expert guidance and continuous encouragement throughout to see that this project rights its target since its commencement to its completion.

We would like to express deepest appreciation towards **Dr. P. Gunasekaran**, Vice Chancellor, VIT BHOPAL UNIVERSITY, **Dr. Manas Kumar Mishra**, Dean of Department of Computer Science Engineering and **Dr. Ajit Kumar**, Project Coordinator whose invaluable guidance supported us in completing this project.

At last we must express our sincere heartfelt gratitude to all the staff members of Computer Engineering Department who helped me directly or indirectly during this course of work.

Meeraj Gawde

Gaurav Kachare

Vishwajeet Mishra

Akshat Nigam

ABSTRACT

This is a new initiative for extracting critical information such as all the host and destination IPs in the form of sessions and some extra information about them such as geo location, no. of TCP and UDP packet from each IP, form a pcap file in the form of sessions in each transmission of data.

Our major highlight of this program is that linkage of nmap for easier access and efficient use of our tool with the passive geo-location support and completely organized network analyzer tool,with developer support.

The aim of this program is to reduce time consumption required by the forensic expert to analyse the pcap file and help him to create proper report.

Contents

Chapter 1

Introduction

This is a new initiative to extract critical information from network traffic which is obtained in the form of a .pcap file via various software such as Wireshark or Network Miner. Basically we have used some predefined python libraries such as scapy, dpkt, argparse, os, sys, and pyfiglet to show all the data transactions in the form of sessions and display the detailed information according to the flags used.

Full content packet analysis provides analysts with the ability to review exactly what has transpired on a network. Analyst neither have to rely on questionable logs nor perform guesswork when determining what data have been transferred. One of the benefits to utilizing full packet captures is the ability to extract specific files that are transferred between host and the network. These files can then be used for more in-depth analysis to determine the true nature of Malware.

Chapter 2

Software Requirements Specification

Python (cross platform).

Wireshark (for capturing pcap file).

Command Prompt/Terminal (for executing the program).

Chapter 3

Background

There are some software such as:-

Foremost- Well known forensic tool for file carving.

PhotoRec- Used for deleted photo extraction(file carving).

EtherApe- is a packet sniffer/network traffic monitoring tool, developed for Unix.

But these apps were unable to recover files and data from the network or unable to work with multiple platforms and no network monitoring or no GUI version is available or requires heavy specification.

Chapter 4

System Design

In this program we just take a .pcap file (already existing or taken at same time) simply downloaded from Wireshark or Network Miner. Now, open the terminal in any operating system and just type the name of python file name and the mention which flag you want to use initially you may type help for getting general overview of the tool.

Using this tool we can perform following tasks,
1) Accept a .pcap file.
2) Find total number of packets, including separate tcp and udp packets.
3) find the geo-location.
4) All host and Destination IPs from which files are downloaded during the sessions.

Chapter 5

Project Planning

08/08/2019 Idea proposed.
16/09/2019 Analyzed existing work’s problem.
10/10/2019 First prototype with geo-location.
22/10/2019 Second prototype with host and destination analyzer.
30/10/2019 Completed the project with banner and arg-parser.

Chapter 6

Implementation

1) userDownload- It captures http-get request from tcp packets and finds source and destination ip.

2) geoLoc- Finds the geo- location of host and source in a particular session.

3) countPac- Counts total number of packets in pcap.

4)Nscan- Provides access to all functionality of nmap tool.

Chapter 7

Applications

1) In Digital Forensics, for accessing ephemeral data.

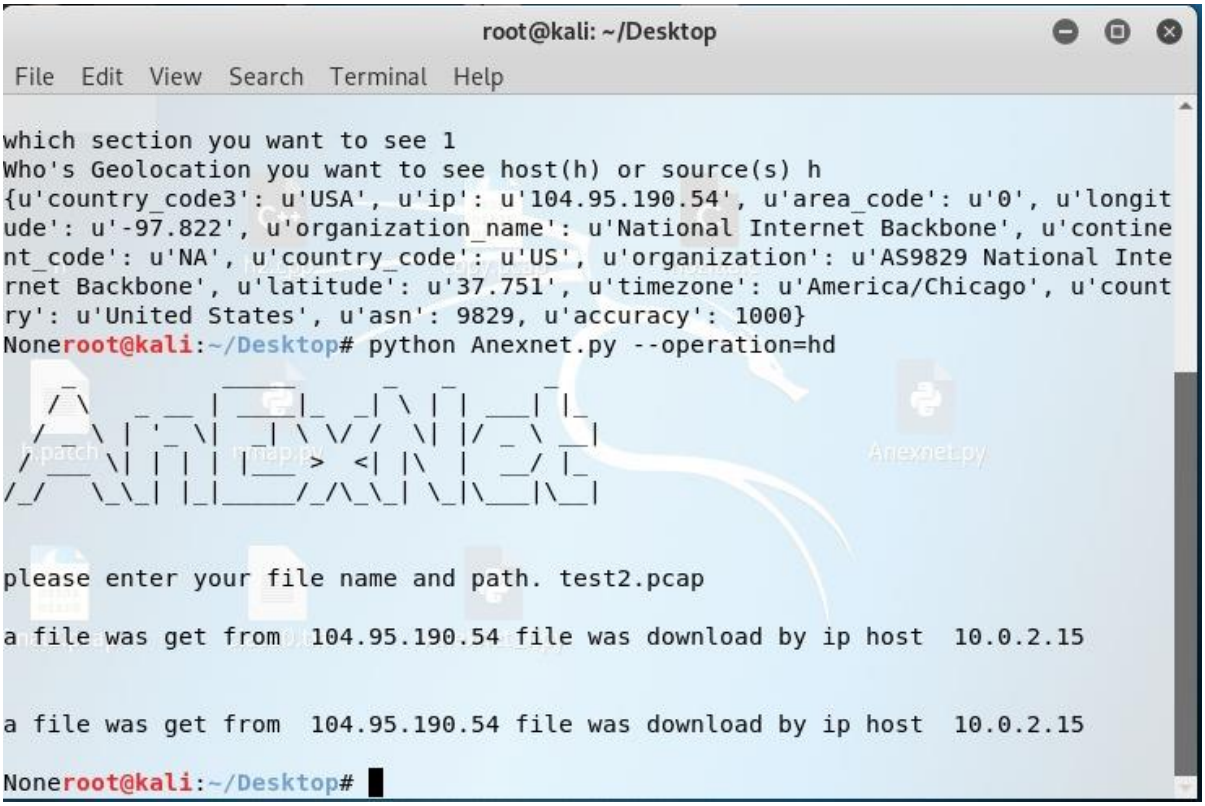
2) Identify security threats.

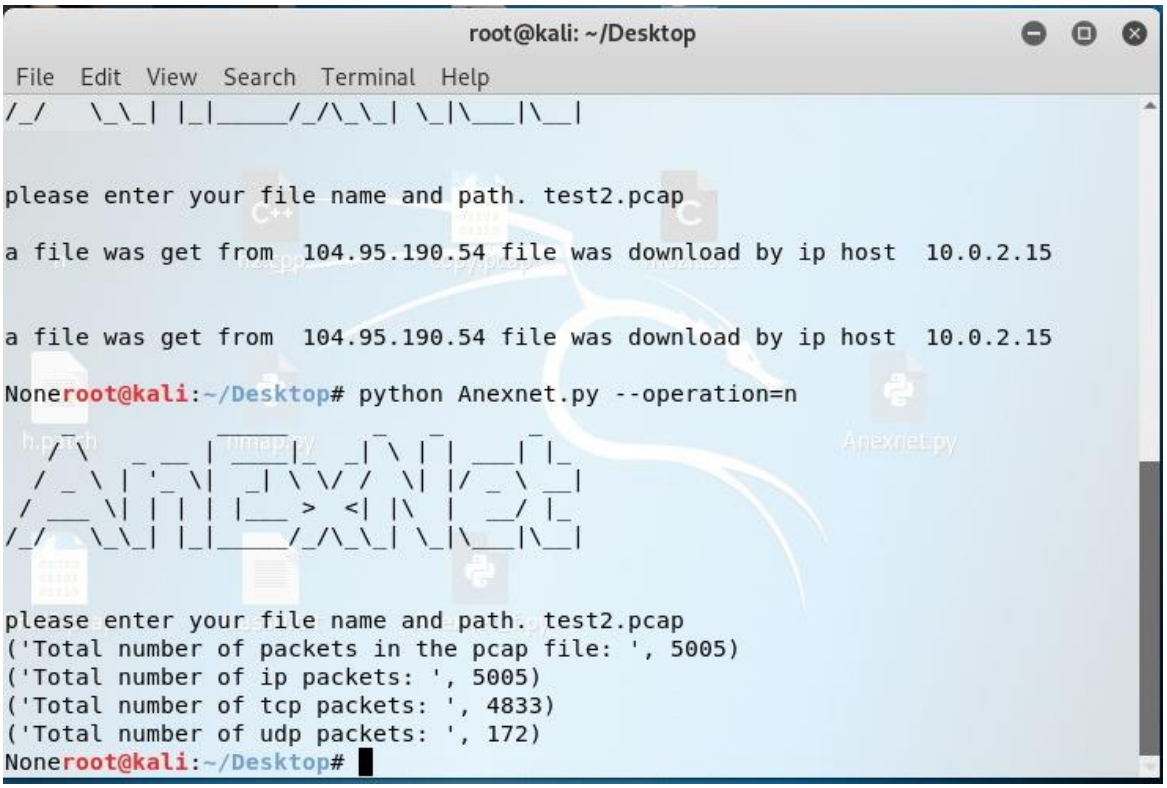
3) Identify what applications/protocols are running on the network.

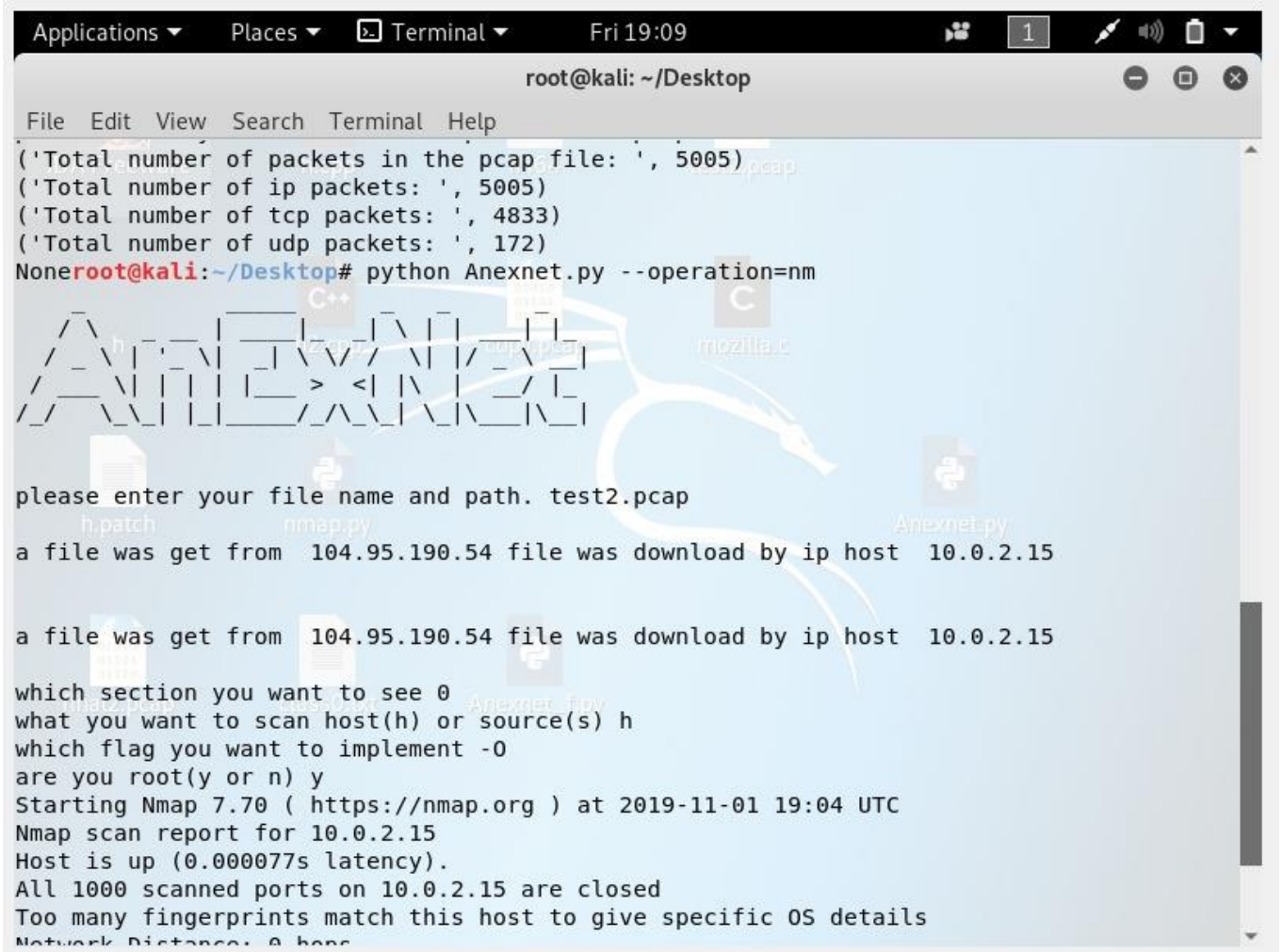
4) Monitor client to server network traffic.

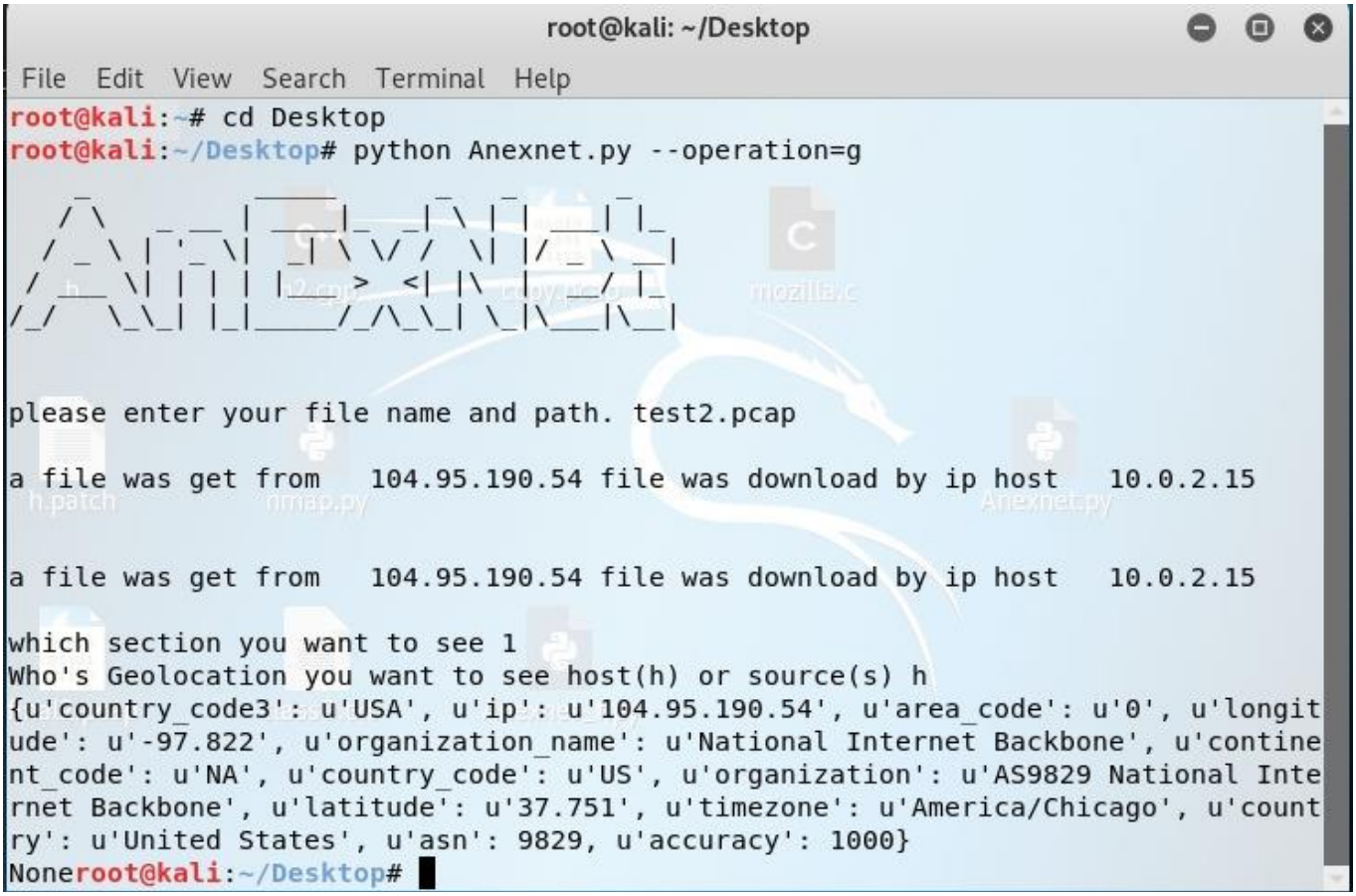
Chapter 8

Screenshots of Project






Applications
Places
Terminal
Fri 19:09
root@kali: ~/Desktop
File Edit View Search Terminal Help
('Total number of packets in the pcap file: ', 5005)
('Total number of ip packets: ', 5005)
('Total number of tcp packets: ', 4833)
('Total number of udp packets: ', 172)
Noneroot@kali:~/Desktop# python Anexnet.py --operation=nm
please enter your file name and path. test2.pcap
a file was get from 104.95.190.54 file was download by ip host 10.0.2.15
a file was get from 104.95.190.54 file was download by ip host 10.0.2.15
which section you want to see 0
what you want to scan host(h) or source(s) h
which flag you want to implement -O
are you root(y or n) y
Starting Nmap 7.70 (https://nmap.org) at 2019-11-01 19:04 UTC
Nmap scan report for 10.0.2.15
Host is up (0.000077s latency).
All 1000 scanned ports on 10.0.2.15 are closed
Too many fingerprints match this host to give specific OS details


root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~# cd Desktop
root@kali:~/Desktop# python Anexnet.py --operation=g
please enter your file name and path. test2.pcap
a file was get from 104.95.190.54 file was download by ip host 10.0.2.15
a file was get from 104.95.190.54 file was download by ip host 10.0.2.15
which section you want to see 1
Who's Geolocation you want to see host(h) or source(s) h
{u'country_code3': u'USA', u'ip': u'104.95.190.54', u'area_code': u'0', u'longit
ude': u'-97.822', u'organization_name': u'National Internet Backbone', u'contine
nt_code': u'NA', u'country_code': u'US', u'organization': u'AS9829 National Inte
rnet Backbone', u'latitude': u'37.751', u'timezone': u'America/Chicago', u'count
ry': u'United States', u'asn': 9829, u'accuracy': 1000}
Noneroot@kali:~/Desktop#

Chapter 9

Conclusion and Future Scope

Extraction of critical information from a .pcap file is very difficult and Consumes lots of time, so using our tool , any security analyst can easily extract and analyse the .pcap file at one place.

It can be linked with other forensic tools to automate the whole process of Information analysis as well as information gathering.

Chapter 10

Bibliography

1] https://en.wikipedia.org/wiki/File_carving

2] https://www.techopedia.com/definition/20663/memory-dump

3] https://www.motadata.com/blog/netflow-traffic-monitoring/

4] https://blogs.cisco.com/security/network-based-file-carving