Department of Computer Science and Engineering

Experiential Learning Report

"Python Cybersecurity— Network Tracking using Wireshark and Google Maps"

Course Code: 22EM106

Course Title: INTRODUCTION TO CYBER SECURITY

Submitted by:

1. **VEDANTH SRIRAM (RVCE22BEC094)**
2. **SHRAVAN V (RVCE22BEC179)**
3. **AVIRAL JAIN(RVCE22BEC037)**

2022-2023

Staff Incharge:-

Dr. Mohana

Assistant Professor

Dept of Computer Science and Engineering

RV College of Engineering

ACKNOWLEDGEMENT

We are indebted to our faculty**, Dr.Mohana,** Assistant Professor, CSE Dept, RVCE, for her wholehearted support, suggestions and invaluable advice throughout our Project work.

Our sincere thanks to **Dr. Ramakanth Kumar P.**, Professor and Head, Department of Computer Science and Engineering, RVCE for his support and encouragement.

Lastly, we take this opportunity to thank our **family** members and **friends** who provided all the backup support throughout the project work.

TABLE OF CONTENTS

1.Introduction

Cybersecurity refers to a set of techniques used to protect the integrity of networks, programs and data from attack, damage or unauthorized access. The use of cyber security can help prevent cyber-attacks, data breaches, and identity theft and can aid in risk management. So when talking about cybersecurity, one might wonder "*What are we trying to protect ourselves against?*" There are three main aspects we are trying to control, name:

- Unauthorised Access
- Unauthorised Deletion
- Unauthorised Modification

These three terms are synonymous with the very commonly known CIA triad which stands for Confidentiality, Integrity, and Availability. The CIA triad is also commonly referred to as the three pillars of security and most of the security policies of an organization are built on these three principles.

Cybercrime is any unauthorized activity involving a computer, device, or network. The three types are computer-assisted crimes, crimes where the computer itself is a target, and crimes where the computer is incidental to the crime rather than directly related to it. Cybercriminals usually try to profit off of their crimes using a variety of tactics, including: Denial of Service, Malware. Man in the middle, Phishing etc.

Cyber Security experts employ different tactics to secure computer systems and networks. Some of the best practices include:

- Using two-way authentication
- Securing passwords
- Installing regular updates
- Running antivirus software
- Using firewalls to disable unwanted services
- Avoiding phishing scams
- Employing cryptography, or encryption
- Securing domain name servers, or DNS

In this project, we are demonstrating one of the basic activities that involve tracking of sites visited by a user. This is achieved by looking at the network packets that are sent over the internet to various locations based on the IP address of source and destination. 'Man in the Middle' attack is achieved by capturing such packets from the origin location, making a copy of it and then forwarding the same packet to the destination. The user will be clueless about this activity but the data that is being sent across is being snooped by a middleware component. Tracking such packets also helps a cybercriminal know the frequent network destinations to which the user interacts.

The project uses an application called 'WireShark' which helps captures the network packets that are sent out from the origin system. These packets are then stored in a special file. A custom application, written in Python, then opens this saved packet file, does a reverse lookup of the IP address and converts to geo-location (latitudes/longitudes). The output from the Python program is then provided as input to Google Maps, which then pictorially shows the actual origin and destination locations of the network packets.

2. Problem Statement

Due to very large bandwidth provided by ISP, people generally allow a lot of traffic through without even analyzing or ensuring to whom the data is being received by

Without the user's knowledge, a third-party user might be capturing the data packets being transmitted, makes a duplicate copy and sends it to the destination. By knowing the frequent destinations with which user interacts with, they can extract these data and use it for malicious purposes

3. Objectives

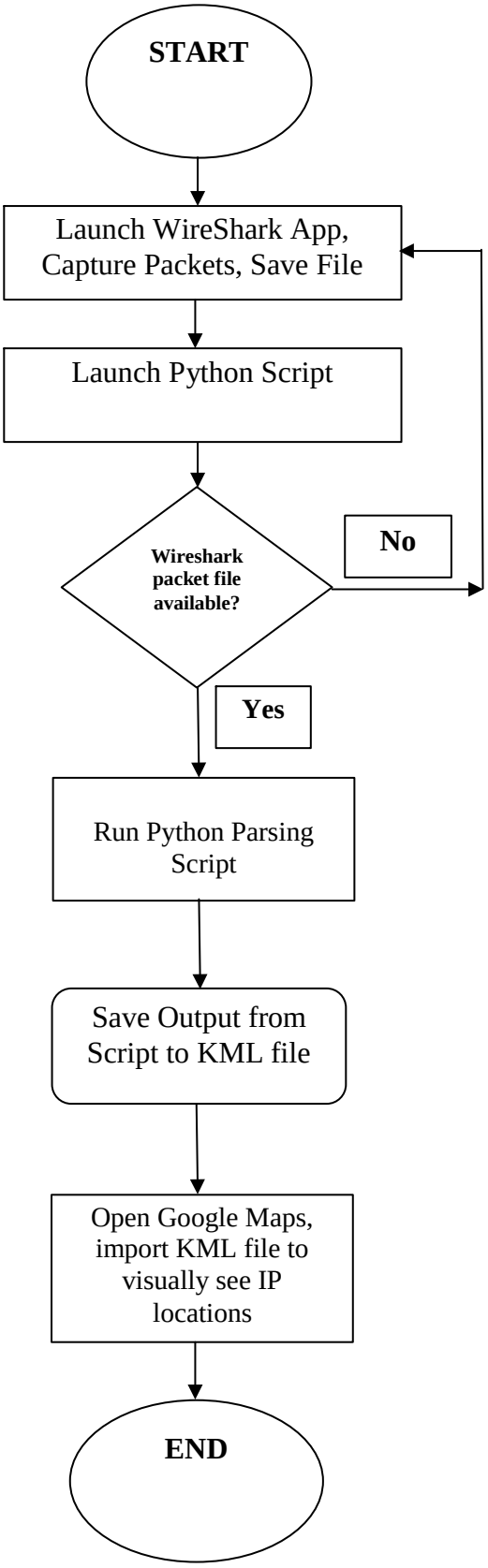
The objective of our simulation is to observe the destination of the data packets sent by the user. If the data packets reaches any destination not specified by the user, appropriate measures can be taken place

4. Literature Survey

AUTHOR	PAPER TITLE	PUBLICATION DETAILS	REMARKS
Vanya Ivanova *Tasho Tashev* *Ivo Draganov*	DETECTION OF IOT BASED DDoS ATTACK BY NETWORK TRAFFIC ANALYSIS	**International Journal of Circuits, Systems and Signal Processing**,2022	• An optimized feedforward neural network model is proposed for detection of IoT based DDoS attacks by network traffic analysis Testing over the Bot IoT dataset reveals that developed models are applicable using 8 or 10 features and achieved discrimination error of 4.91.10-3%.
Himanshu Gandhi *Vinay Ribeiro*	PACKET BATCHING IN NETWORK TRAFFIC ANALYSIS	14th conference on COMSNETS,BANGALORE ,2022	•Packet switching can reduce system resource consumption for botnet detection
Kovtsur Maxim *Potemkin Pavel*	RESEARCH OF WIRELESS NETWORK TRAFFIC ANALYSIS	13th International Congress on UMT,Brno,2021I	•Wireless network traffic can be analysed using python programming tools

Sheetal Thakare Anshuman Pund M A Pund	NETWORK TRAFFIC ANALYSIS: IMPORTANCE,TECHNIQUES	3RD International Conference on CES, Coimbatore,2018	•Reviewing the importance and benefits of network traffic analysis
Fabian Popa	NETWORK TRAFFIC VISUALISATION	Seminar Innovative Internet-Technologien und Mobilkommunikation, WS 2018/2019	•Implementation of converting network traffic file to a visual presentation and methodology
H. Kim, H. Lee and H. Lim	Performance of Packet Analysis between Observer and WireShark	*22nd International Conference on Advanced Communication Technology (ICACT)*, Phoenix Park, Korea (South), 2020	Network Forensics refers to a technology that analysis all actions are taken on the network and analysis and responds to attacks through packet analysis.
K. M. Majidha Fathima and N. Santhiyakumari	A Survey On Network Packet Inspection And ARP Poisoning Using Wireshark And Ettercap	*International Conference on Artificial Intelligence and Smart Systems (ICAIS)*, Coimbatore, India, 2021	The network traffic is being interpreted by wireshark.
G. Sasi, P. Thanapal, V. S. Balaji, G. V. Babu and V. Elamaran	A Handy Approach for Teaching and Learning Computer Networks using Wireshark	*Fourth International Conference on Inventive Systems and Control (ICISC)*, Coimbatore, India, 2020	Elucidates a few imperative views behind computer networks theory with a firsthand approach.

5. Design And Implementation



This process has the following discrete steps to be followed:

- Wireshark data capture of network packets
- Python Data Processing Script transformation of captured packets
- Visual depiction of Network traffic using Google Maps

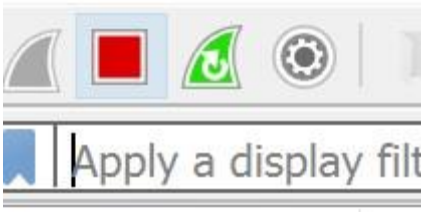
Wireshark Data Capture:

Wireshark package can be downloaded (from https://www.wireshark.org) and installed from the internet onto the host system. The flow starts with launching the Wireshark application. Upon launching the Wireshark application, the GUI will have options to start / stop the capture of packet. WS application also has options to export the captured data in various formats. Ensure that the system is now connected to the internet via LAN or WLAN. Do note the IP address allocated to this system as it would help determine the origin of packets.

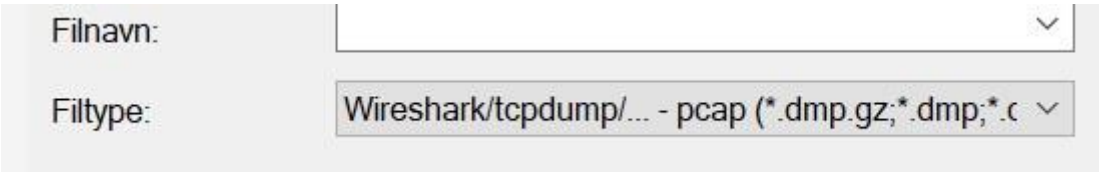
Now launch some other application such as a Browser. Click the 'Start' capture button in the WS application. Using the browser window, navigate to different sites. You can choose sites that are local to the country as well as other international sites. After a few browsing activities, navigate back to the WS application and 'Stop' the packet capture. Choose the 'Export' menu from the WS application to save the captured packets in a 'pcap' file format.

Ethernet Interface with traffic

Start / Stop capture of traffic in WS application



Saving of Captured data in WS application



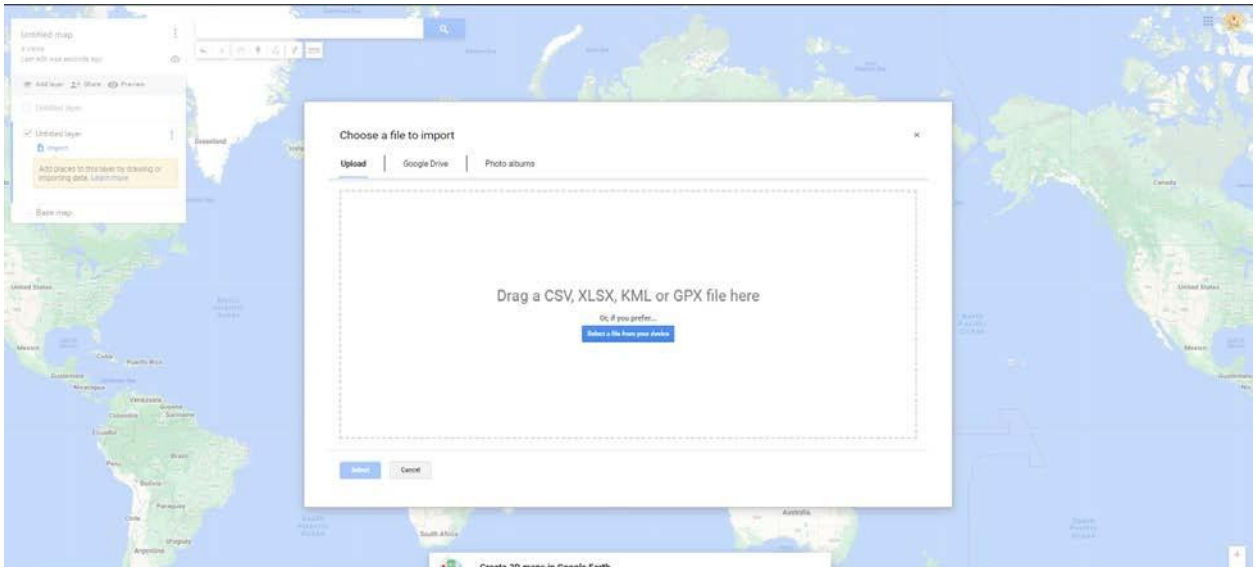
Python Data Processing Script:

Ensure that the local system has the required software to run Python programs. Also in the HOME directory of the project, download and store the 'GeoLiteCity' database as this will be used to translate a IP address into a Geo location (longitude/latitude). The database can be downloaded from: https://github.com/mbcc2006/GeoLiteCity-data.

From within the Python Development environment, run the Python script. It will prompt the user to select the ‘pcap’ file that was originally saved from the above step. After selecting the ‘pcap’ file, the script has the logic to parse the ‘pcap’ file , extract the IP encoded packet information, do a reverse lookup of the IP using the ‘GeoLiteCity’ database to transform the packets into a Geo Location data set. The output of this program is saved into a ‘kml’ file after parsing through the entire ‘pcap’ file.

Visual Depiction of captured packets:

Once the Python script has generated the ‘.kml’ file, now open Google Maps, using the following url: https://www.google.com/mymaps. Import a new layer onto the Google Maps, by selecting the ‘.kml’ file generated from the Python script. See below pic on how to import the saved file into Google Maps.



Once the .kml file is processed by Google Maps it will now visually depict the origin and destination of IP addresses on the world map, so that it can be visually seen as to where the IP packets were being sent to from the host system.

6. Simulation Results and Analysis

(Detailed results screenshots, Explanation, Analysis)

Do see below a pictorial representation of the captured data based on some browser navigation from the host system. It is clear from the picture that several packets of information have originated from India location and have been sent to various locations in US, Europe and Japan.

This pictorial representation is based on the sites visited via the browser. The operating system on the host (Windows) also constantly communicates with servers outside the country. Hence it can be seen that some of the packets of information have be sent to US (Washington) as well.

Using available applications like Wireshark, Google Maps and a small Python script it is quite easy to snoop on the network packets sent from the host system and graphically map them. For a cybercriminal, who is well versed in network stacks, a much more complex program can be written to snoop on these packets and use them for mal-practice purposes , thereby creating a cyber security risk.

7. Conclusions

In the modern world where internet connectivity has become ubiquitous, it is very much essential for a user to be cautious on securing his/her computer system through all cyber secure means to prevent data snooping/data theft. The user should always use certified copies of software, should NOT install any unknown/unsigned/unlicensed software, should have malware protection software installed and should show utmost caution in not visiting unwanted phishing sites on the internet that might install malware/virus software on the host system.

8.References

1.Vanya Ivanova, Tasho Tashev, Ivo Draganov,**DETECTION OF IOT BASED DDoS ATTACK BY NETWORK TRAFFIC ANALYSIS,** International Journal of Circuits, Systems and Signal Processing**,**2022

2.Himanshu Gandhi,Vinay Ribeiro, **PACKET BATCHING IN NETWORK TRAFFIC ANALYSIS**
14th conference on COMSNETS,BANGALORE,2022

3. Kovtsur Maxim, Potemkin Pavel,**RESEARCH OF WIRELESS NETWORK TRAFFIC ANALYSIS**
13th International Congress on UMT,Brno,2021

4.Sheetal Thakare, Anshuman Pund, M A Pund,**NETWORK TRAFFIC ANALYSIS: IMPORTANCE,TECHNIQUES**
3RD International Conference on CES, Coimbatore,2018

5. *Fabian Popa*, NETWORK TRAFFIC VISUALISATION, **SEMINAR INNOVATION INTERNET-TECHNOLOGY AND MOBILE COMMUNICATION**, WS 2018/2019

6. G. Sasi, P. Thanapal, V. S. Balaji, G. V. Babu and V. Elamaran, "A Handy Approach for Teaching and Learning Computer Networks using Wireshark," *2020* **22nd International Conference on Advanced Communication Technology (ICACT), Phoenix Park, Korea (South), 2020**

7. K. M. Majidha Fathima and N. Santhiyakumari, "A Survey On Network Packet Inspection And ARP Poisoning Using Wireshark And Ettercap," **2021*International Conference on Artificial Intelligence and Smart Systems (ICAIS), Coimbatore, India, 2021***

8. H. Kim, H. Lee and H. Lim, "Performance of Packet Analysis between Observer and WireShark," *2020* **Fourth International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 2020**