

DETECTION OF DOS &DDOS ATTACKS

A Project Work Synopsis

Submitted in the partial fulfillment for the award of the degree of

**BACHELOR OF ENGINEERING
IN
COMPUTER SCIENCE**


Submitted by:

**K. SAI TARAK
18BCS2406**

**M.KASI REDDY
18BCS2360**

Under the Supervision of

DEEPTI SHARMA



formatting mistakes



**CHANDIGARH
UNIVERSITY**

Discover. Learn. Empower.

**CHANDIGARH UNIVERSITY, GHARUAN, MOHALI -
140413, PUNJAB**

January-May, 2021

Table of Contents

Title Page

Abstract

- 1. INTRODUCTION**
- 2. FEASIBILITY STUDY**
- 3. METHODOLOGY**
- 4. MODULE AND TEAM MEMBER WISE DISTRUBUTION OF WORK**
- 5. INNOVATIONS IN PROJECT**
- 6. SOFTWARE REQUIREMNETS**
- 7. BIBLIOGRAPHY**

ABSTRACT

Our project concerns the field of Cyber Security and aims at detecting DOS or DDOS attacks. Although we had developed the project with the Institute Gateway in our mind, the software works pretty well with any other network or any personal computer. The main aim of our team was to build a software from scratch that is light, gives the user real time information about the said network and could work independently. The project presented below is developed with the sole motive of detecting a DOS attack by distinguishing it from legitimate network traffic efficiently. However, we aim at improving our software with the help of various deep learning techniques while keeping our software light and fast.

1. INTRODUCTION:

Network Behavior Anomaly Detection (NBAD) affords a method to network security threat detection. It is a balancing technology to systems that determine security threats based on supported packet signatures. NBAD is the process of endlessly watching a network for unusual events or trends. NBAD is an integral part of network behavior analysis (NBA), that offers security in addition to the services provided by ancient anti-threat applications like firewalls, intrusion detection systems, antivirus computer code, and spyware-detection computer code. Laptop security has become a necessity because of the proliferation of knowledge technologies in the standard of living. The mass usage of processed systems has given rise to crucial threats like zero-day vulnerabilities, mobile threats, etc. Despite analysis within the security domain having hyperbolic considerably, nonetheless, the threat often seems to be mitigated. The evolution of laptop networks has greatly exacerbated laptop security considerations, notably web security in today's networking setting and advanced computing facilities. Though web Protocols (IPs) weren't designed to position a high priority on security problems, network directors nowadays have to be compelled to handle an outsized style of intrusions made by people with malicious intents and huge botnets.

In educational analysis, however, anomaly detection approach is perceived to be additionally powerful because of its higher potential to deal with novel attacks as compared to misuse-based strategies. According to threat Report of the Symantec web Security, there have been over three billion attacks of malware was reported in 2010 and therefore the variety of Denial-of-Service attacks increased hyperbolically by 2013 (Symantec web security threat report, 2014). As explicit in Verizon's knowledge Breach Investigation Report 2014, 63,437 security breaches were launched by hackers distributed throughout the world. The world State of knowledge security Survey 2015 (The international State of knowledge Security Survey, 2015) found a rise in the number of such incidents. Therefore, the detection of network attacks has given the much priority these days. Additionally, the experience needed to commit cybercrimes has diminished because of simply offered tools. Anomaly detection is a crucial knowledge analysis task that detects abnormal or malicious knowledge from a given dataset.

2. FEASIBILITY STUDY

Innovative cyberattacks are featured by several layers, varieties and stages, with the goal of duplicitous the monitors. Existing of anomaly detection systems search typically traffics and logs alone for proof of attacks however ignore any analysis regarding attack processes. As an example, the traffic observation strategies will solely detect the attack flows roughly however fail to provide us with detailed information about the attack. Most security observance systems utilize a signature-based approach to observe threats. They typically monitor packets on the network and appearance of patterns within the packets that match their information of signatures representing preidentified well-known security threats. NBAD based systems are significantly useful in the detection of security threat vectors in two instances where signature-based systems can't be used:

- (i) new zero-day attacks, and
- (ii) once the threat traffic is encrypted as command and management channels.

Example: Botnets and Spams.

With the entrance and volatile growth of the world wide web and ecommerce environments, adaptive/automatic network/service intrusion and anomaly detection in wide space knowledge networks and ecommerce infrastructures is quick gaining vital analysis and is of global importance.

DoS Attack Result: We have set up a test environment to understand whether the proposed DoS attack is successful or not, and the environment consists of a single OpenFlow switch, a controller, and two hosts for network communications. We use the software based OpenFlow switch implementation for the OpenFlow switch [3], and it is installed on an independent Linux host, and we set the maximum flow rules for this switch as 1,500, which is the same configuration for HP 5406zl switch

TECHNICAL FEASIBILITY: This aspect concentrates on the concept of using Computer Meaning, “Mechanization” of human works. Thus, the automated solution leads to the need for a technical feasibility study.

The focus on the platform Network & users for that S/W.

The proposed system doesn't require an in-depth technical knowledge as the system development is simple and easy to understand. We have used python as a tool and different libraries for packet sniffing, TKinter library for GUI in python to provide the user

3. METHODOLOGY

In our project, we make use of the Scapy Library of Python to sniff network packets. The Tkinter Library is used to make the GUI in python to provide the user with a more interactive interface.[4] The Matplotlib Library is used to plot the pie chart, the bar graph, and the time plot. The Math Library is used to do some mathematical formatting and the Time library is used to get the current time. When we run the program, the main function of the code is executed first which results in a GUI popping up which consists of a column span of two using a Label Widget and a drop-down menu placed at grid position (3, 2) containing three options: 1. Five minutes, 2. Ten minutes, 3. Fifteen minutes using an Option Menu widget. The GUI also consists of a start button placed at grid position (2, 1) with a row span of 2 using a Button widget.

On selecting the time from the given options, and clicking on the Start button beside it, the program runs the start function which has been passed as an argument of the button widget B. The start function runs a loop for the amount of time that the user had selected in the GUI. In each execution of the loop, the sniff function that has been imported from the Scapy Library captures a single network packet using the parameter count = 0 and searches for the protocols that are present in that packet and increases the number of packets in that protocol by one if that protocol is present in the packet. In this project we are sniffing packets with respect to six protocols namely: TCP, UDP, DNS, IP, FTP, and HTTP. After updating the count for each protocol, the program plots the pie chart using the above information showing the percentages of packets of the total number of packets with respect to each protocol.

To put our program to test, we launched an artificial DOS attack onto our own computer and checked if our program worked correctly.

We can launch an artificial attack using software Switch Blade by following simple steps:

- Open the command prompt/terminal on the computer
- Enter the following command: ipconfig
- Copy the default gateway address
- Open Switch Blade GUI and type the address in the URL section.
- To start, click on the button run.

in order to the attack to be more effective, we must attack the target computer with the pings from another computer. The overhead attack can be used to attack the routers, web servers etc.

4. MODULE AND TEAM MEMBER WISE DISTRUBUTION OF WORK

Team Members wise Distribution of work:

IN our team we are two members each of us were allotted with works

We have learned about DOS and DDOS attacks, how they have been attacked and things we have to take care in detection of it

SAI TARAK working on networks and different types of ports, TCP 3-way handshake

KASI REDDY working on malwares and on software Spyder IDE, different types of libraries

5. INNOVATIONS IN PROJECT

Our project is at the present moment in the early stages of its development. As of now our project is tailored to perform only those tasks that have been discussed above. It is yet to reach its full potential. The primary aspects of the project which we have decided to work upon are:

- Faster computation speeds.
- Lighter and more efficient software.
- Ability to detect the name of the protocol that had been used to launch the attack.
- Large scale implementation of our project in industrial servers.
- For PC users, we have come up with an idea to tailor our software according to their daily needs. Internet usage is not the same throughout the day and often varies widely across the days of the week. So, with the help of Artificial Intelligence we have attempted to study the daily and timely internet usage patterns of users and as a result be better able to differentiate between legitimate requests and attacks.

But, with respect to the cyber security community as a whole, as technology is increasing day by day, new methods and various machine learning techniques perpetually plan to improve the information discovery process. Given the actual fact that web traffic doubles every year and network traffic are increasing at a quick rate creating it a difficult task to watch a network in real-time. Existing anomaly detection techniques are largely for watching one system or one network by winding up native analysis for attacks. Hence, between instances of such standalone anomaly detection techniques, no communication and interaction exist. Certainly, such an answer won't be able to sight subtle and extremely distributed attacks. Thus, for the safety of enormous networks and huge IT ecosystems (i.e., cloud services), cooperative techniques are very economical that comprise many monitors that act as sensors and collect knowledge. Due to the inconvenience of implementations of cooperative techniques like CIDSs (Collaborative Intrusion Detection Systems), future analysis efforts are necessary for in-depth quantitative analysis with state-of-the-art network infrastructure.

6. SOFTWARE REQUIREMENTS

The software tools used in our project are:

- The Anaconda Installation of Python
- The Spyder IDE

We have used the Anaconda Installation of Python since it comes pre-installed with most of the basic python libraries such as Pandas, Matplotlib, NumPy, etc. Another benefit is that the Anaconda installation comes with the Spyder IDE is a very useful tool since it helps us visualize the results of any part of our program code inside the same terminal in its kernel without having to run the whole code. It proves to be a very useful tool when it comes to visualizing Data Science results.

The Python libraries used in this project are:

- The Scapy Library
- The Tkinter Library
- The Matplotlib Library
- The Math Library
- The Time Library

7. BIBLIOGRAPHY

- Petersen, B. and Chung, E., Broadcom Corp, 2009. Network activity anomaly detection. U.S. Patent Application 12/015,387.
- Garcia-Teodoro, P., Diaz-Verdejo, J., Maciá-