IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

AN EASY-TO-USE MECHANISM TO PREVENT DDOS AND ARP SPOOFING NETWORKING ATTACKS

Thalari Ravindra[1], Dr. V Umarani[2]

[*1]Student, M.Tech(Computer Networks and Information Security), School of Information Technology, JNTU Hyderabad, Hyderabad, India

[*2]Professor of IT, School of Information Technology, JNTU Hyderabad, Hyderabad

ABSTRACT: System hacks, data theft, and denial-of-service assaults meant to interrupt services are just a few of the various ways that computer networks can be attacked. Numerous attacks on computer networks have a detrimental effect on the infrastructure and its application services. From a cyber-offensive and defensive standpoint, There are various tools available for creating and injecting custom malicious packets into networks, as well as exploiting operating system and application vulnerabilities. But practitioners with a limited understanding of networking fundamentals and students who are just beginning their studies may find it difficult to manage these tools.The scapy library, which is used to process and inject network packets, was utilized in its development and is written in Python. The effectiveness and usability of the application will be assessed throughout a testing phase.Active DDoS attacks can be challenging to stop and may harm legitimate users. For this reason, it's crucial to adopt a preventative stance. We should develop an emergency DDoS incident response plan in addition to the preventive steps listed below because even the finest defenses can occasionally be overcome by clever attacks. As packets enter your system, assess them using various criteria and filter out those that may be harmful. A DDoS protection system can identify content with malicious intent that appears to be legitimate.

Keywords: denial-of-service; computer networks; DDoS attacks preventive steps; protection system.

1. INTRODUCTION

Using a DDoS attack, a hacker can saturate a network or server with fake traffic. When connectivity is disrupted and resources are overloaded, the system is unable to handle legitimate user requests. Services stop working, causing the target business to have extended downtime, lose money, and have unhappy customers. Any attempt at a DDoS attack must be stopped by network security. Being able to spot a DDoS early on is essential to limiting the blast radius because an attack only has an impact if a hacker has time to accumulate requests. Keep in mind that not all DDoS assaults include heavy traffic. An attack that is brief and low in volume frequently passes These assaults, though, might be a ruse or a test for a more risky breach. As a result, spotting a low-volume attack is just as important as spotting a full-blown DDoS.

1.1 OBJECTIVE OF THE PROJECT

The psychology and motivations underlying DDoS assaults differ. They include monetary or economic gains, retaliation, ideological convictions, cyberwarfare, or even just for one's own fun.

This is frequently made worse by business owners' misguided notion that their organization is a tiny fish in a vast ocean. Unfortunately, IP spoofing can affect anyone. Without the proper instruction or tools, a reasonably experienced attacker may get over your defenses and have access to your data whenever they want. The best way to secure your company is to be aware of all common types of spoofing attacks and to take action to keep protected from them.

2. LITERATURE SURVEY

2.1 A taxonomy of DDoS attack and DDoS defense mechanisms:

Authors: J. Mirkovic and P. Reiher

The issue of distributed denial-of-service (DDoS) is escalating quickly. Both the number and variety of attacks and defense strategies are overwhelming. In order to help researchers better grasp the issue and the available solutions, this paper introduces two taxonomies for categorizing assaults and defenses. The attack classification criteria were chosen to draw attention to commonalities and significant elements of attack techniques that characterize difficulties and guide the development of defenses.

The defensive taxonomy organizes the corpus of existing DDoS countermeasures into categories based on design choices, and it then illustrates how these choices influence the benefits and drawbacks of suggested solutions.

2.2 An easy-to-use mechanism to inject and prevent DDoS and ARP spoofing networking attacks:

Authors: RANA ABUBAKAR 1,2, (Graduate Student Member, IEEE), ABDULAZIZ ALDEGHEISHEM

There are an unparalleled quantity and variety of attacks on computer networks, the bulk of which are distributed denial of service attacks (DDoS). The nature and techniques used in these DDoS attacks are constantly evolving, making detection and administration extremely difficult. Approaches that can efficiently detect and neutralize developing assaults are needed to handle the evolving nature of attacks. In this research, we present a technique that, in addition to detecting the presence of DDoS attacks, also pinpoints the attack's path and launches a mitigation process right after initial detection. An improved SVM classification algorithm combined with SNORT IPS is used in the proposed research to provide DDoS attack protection methods for the entire network. We describe the approach together with experimental findings that demonstrate superior accuracy, exposure, and specificity than standard Snort IPS, Probabilistic Neural Network (PNN), Back Propagation (BP), Chi-square, and PSO-SVM. These findings demonstrate that our approach has an average accuracy rate of 97%.

2.3 An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment:

Authors: AQEEL SAHI1,2, DAVID LAI2

Despite the fact that there are now a lot more cloud projects than there were a few years ago, it is still important and difficult to conduct research on how to guarantee the security and availability of project data, services, and resources. After identity theft, distributed denial of service (DDoS) attacks are the most frequent cybercrime attacks. DDoS TCP flood attacks have the ability to quickly deplete a cloud's resources, eat up the majority of its bandwidth, and harm an entire cloud project. It is crucial to promptly identify and stop such threats in cloud initiatives, especially for eHealth clouds. We introduce a novel classifier system (CS DDoS) in this research for detecting and stopping DDoS TCP flood attacks in public clouds. By classifying incoming packets and making decisions based on the classification findings, the proposed CS DoS system offers a way to secure stored records. The CS DDOS identifies and determines if a packet is normal or comes from an attacker during the detection phase. Malicious packets will not be allowed access to the cloud service during the preventive phase, and the source IP will be blacklisted. Utilizing the different classifiers of the least squares support vector machine (LS-SVM), naive Bayes, K-nearest, and multilayer perceptron, the performance of the CS DDoS system is compared. The results demonstrate that when the LS-SVM classifier is used, CS DDoS produces the best performance. When under assault from a single source, it can detect DDoS TCP flood attacks with roughly 97% accuracy and a Kappa coefficient of 0.89; when under attack from several sources, it can detect them with 94% accuracy and a Kappa coefficient of 0.9. The results are validated using a K-fold cross-validation model before being discussed in terms of accuracy and time complexity.

2.4 A Unified Approach for Forensic Analysis of DDOS Attack in Manet:

Authors: S. Ahmed, S. M. Nirkhi

Without a centralized infrastructure in place, widespread wireless communication is made possible by Mobile Ad Hoc Networks (MANET). The connection is set up in an ad-hoc manner and the network is portable. The MANET architecture speeds up the deployment of new network infrastructure and increases network scalability. However, MANET's advantages come at the expense of lowered security. A typical DDoS attack is a flooding attack, in which the attackers flood the target networks with an overwhelming amount of traffic in an effort to exhaust the target's essential resources. The breach that starts an investigation occurs when an attack on the target system is effective enough to crash or disrupt it. The forensic investigation serves as a source of network evidence and aids in the development of network attack defense and recovery systems. This document discusses a variety of DDoS attack forensics research projects for MANET.

2.5 KeySplitWatermark: Denial of Service Attacks:

Authors: Qijun Gu, Ph.D.

Attacks that cause a denial of service (DoS) have grown to be a serious danger to current computer networks. This article presents a summary of prevalent DoS assaults and key defense methods in the Internet and wireless networks so that readers can better comprehend them. To demonstrate attack principles, we describe in particular host-based and network-based DoS attack methods. DoS attacks are categorized based on their primary assault traits. A survey of current counterattack technologies is also included, along with a look at the main defense technologies now in use and the leading research defense strategies. Finally, the physical, MAC, and network layers of DoS attacks and responses in 802.11-based wireless networks are examined.

3. PROBLEM IDENTIFICATION & OBJECTIVES

3.1 EXISTING APPROACH

If the predefined attack signature and the new request signature match, the signature-based technique will detect the attack; however, if a new signature is received, it will not detect the attack. Similarly, all known attacks will be trained; however, if a new attack is received, the anomaly technique will also not detect the attack. In a DDOS assault, attackers bombard the server with a large number of requests in a continuous stream. The server must deal with all of these requests while ignoring legitimate ones, and as a result, the server may crash.

3.2 PROPOSED SYSTEM

Introduced cumulative entropy-based calculation (CUSUM) to detect attacks to counter this attack. When this window is filled with all IP addresses, the application will calculate CUSUM. If CUSUM has less values than the number of requests, the requests will be regarded as normal. If a large number of requests arrive, the CUSUM value will rise, and the system will sound an attack alarm.

MODULES

❖ 1.Uploading the dataset begins with choosing and uploading the "signature.pcap" file, after which the dataset is loaded.

❖ 2. Improved Cumulative Sum (CUSUM) Algorithm, which uses the CUSUM technique to analyze pcap files In order to determine whether the request is legitimate or malicious, we must examine the CUSUM array.

❖ 3. Time-Based Entropy Detection: This technique monitors once every 10 seconds thus its detection rate will be lower.

❖ 4. Packets comparison graph: CUSUM & time-based attack detection graph shown.

3.3 ALGORITHMS

The CUSUM approach uses a sliding window base, but we can also use a time-based strategy where the monitoring duration will be defined for the request, for instance, the programme will monitor the initial packet and then carry on capturing for the following 10 seconds and store all packets in the vector. After 10 seconds, the CUSUM algorithm will be used to examine the vector to determine the quantity requested. If more requests are made, the vector will have more high values, and the system will sound an alarm for an assault.

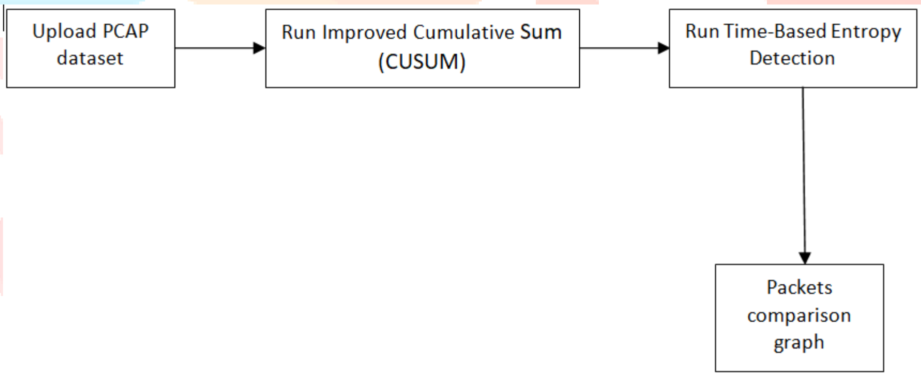
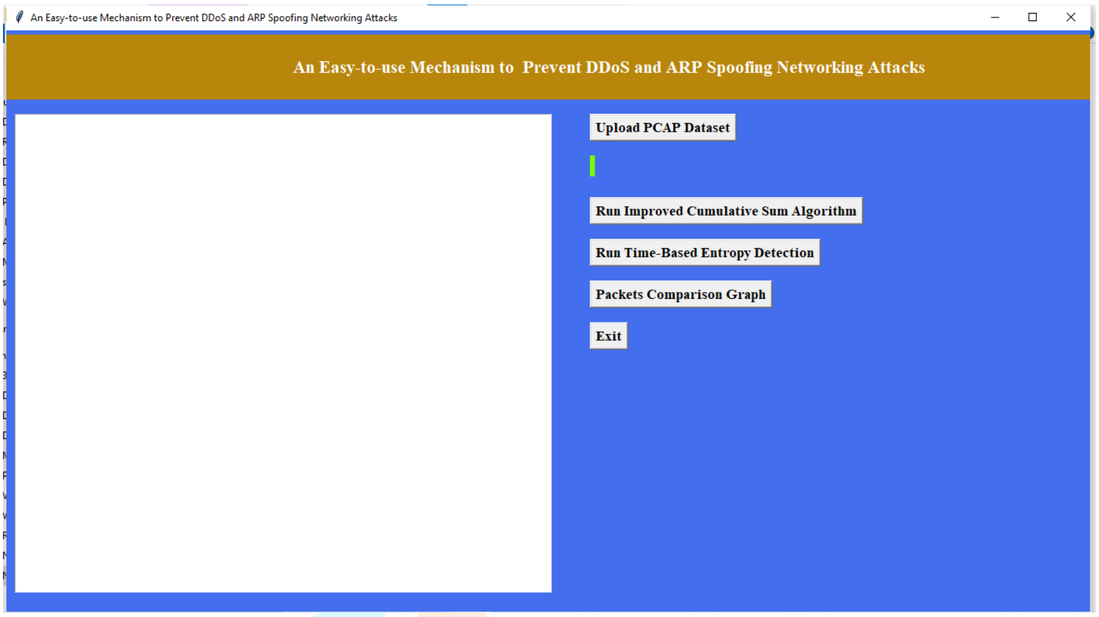

Upload PCAP dataset
Run Improved Cumulative Sum (CUSUM)
Run Time-Based Entropy Detection
Packets comparison graph

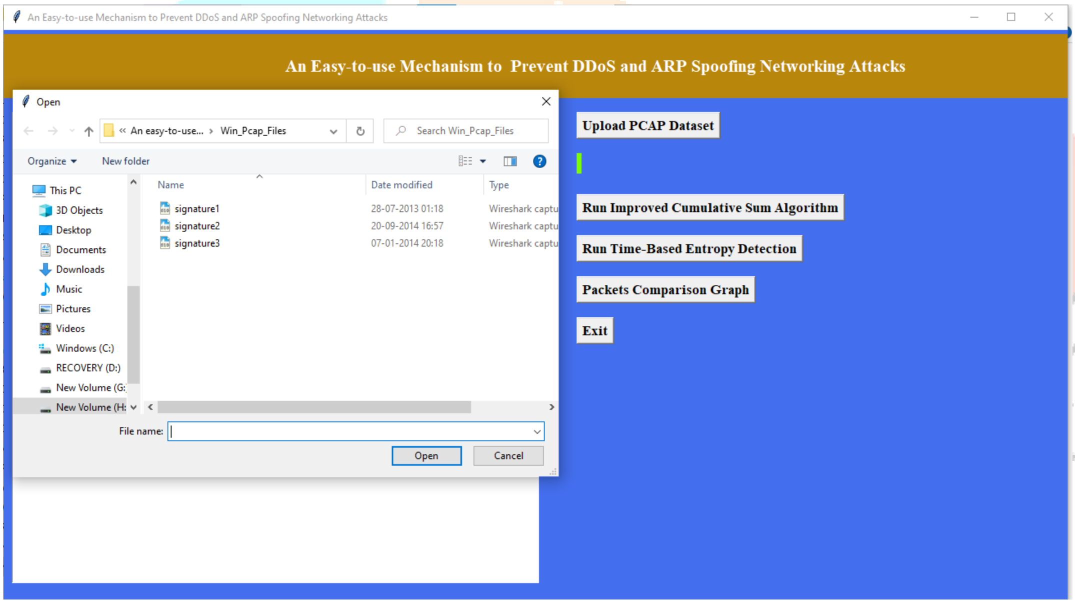
Figure 1. Flow Chart

4. RESULTS & DISCUSSIONS:

To receive the below screen, double click the "run.bat" file


An Easy-to-use Mechanism to Prevent DDoS and ARP Spoofing Networking Attacks
An Easy-to-use Mechanism to Prevent DDoS and ARP Spoofing Networking Attacks
Upload PCAP Dataset
Run Improved Cumulative Sum Algorithm
Run Time-Based Entropy Detection
Packets Comparison Graph
Exit

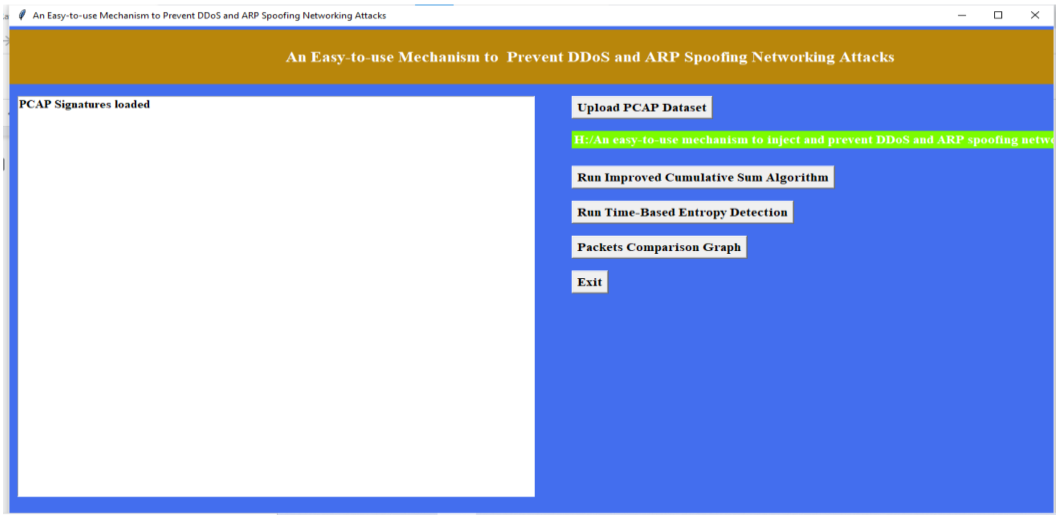
To upload the PCAP file and view the screen below, click the "Upload PCAP Dataset" button in the previous screen.


An Easy-to-use Mechanism to Prevent DDoS and ARP Spoofing Networking Attacks
An Easy-to-use Mechanism to Prevent DDoS and ARP Spoofing Networking Attacks
Open
« An easy-to-use... › Win_Pcap_Files
Search Win_Pcap_Files
Organize
New folder
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Windows (C:)
RECOVERY (D:)
New Volume (G:
New Volume (H:
Open
Cancel
Upload PCAP Dataset
Run Improved Cumulative Sum Algorithm
Run Time-Based Entropy Detection
Packets Comparison Graph
Exit

Name	Date modified	Type
signature1	28-07-2013 01:18	Wireshark captu
signature2	20-09-2014 16:57	Wireshark captu
signature3	07-01-2014 20:18	Wireshark captu

File name: |

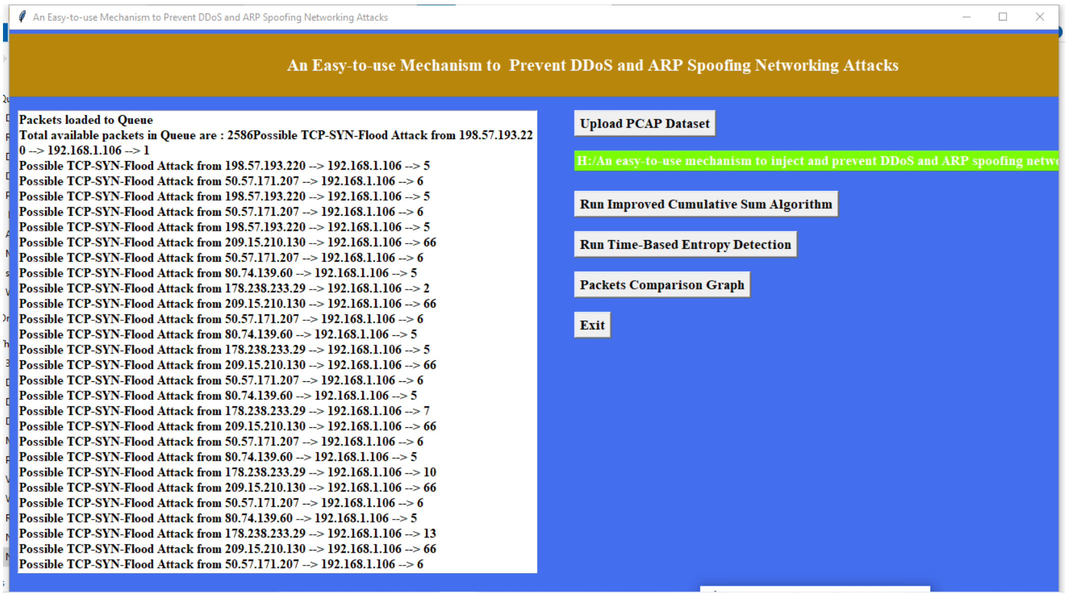
Selecting and adding the "signature.pcap" file on the top screen, then clicking "Open" to bring up the screen below.


An Easy-to-use Mechanism to Prevent DDoS and ARP Spoofing Networking Attacks
An Easy-to-use Mechanism to Prevent DDoS and ARP Spoofing Networking Attacks
Upload PCAP Dataset
Run Improved Cumulative Sum Algorithm
Run Time-Based Entropy Detection
Packets Comparison Graph
Exit

PCAP Signatures loaded

H:/An easy-to-use mechanism to inject and prevent DDoS and ARP spoofing netw

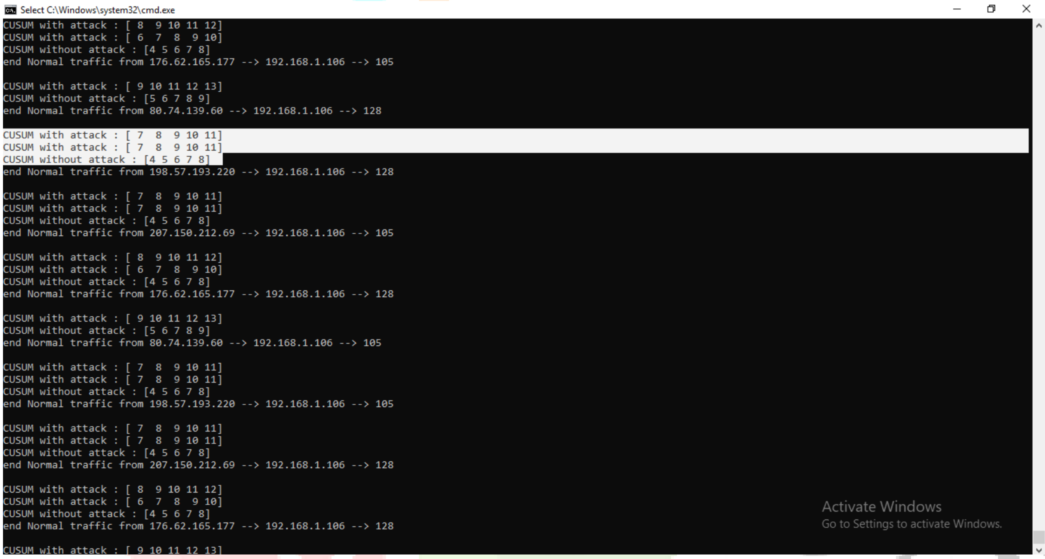
The pcap file is loaded on the screen above. To analyze the pcap file using the CUSUM approach, click the "Run Improved Cumulative Sum (CUSUM) Algorithm" button.


An Easy-to-use Mechanism to Prevent DDoS and ARP Spoofing Networking Attacks
An Easy-to-use Mechanism to Prevent DDoS and ARP Spoofing Networking Attacks
Upload PCAP Dataset
Run Improved Cumulative Sum Algorithm
Run Time-Based Entropy Detection
Packets Comparison Graph
Exit

H:/An easy-to-use mechanism to inject and prevent DDoS and ARP spoofing netw

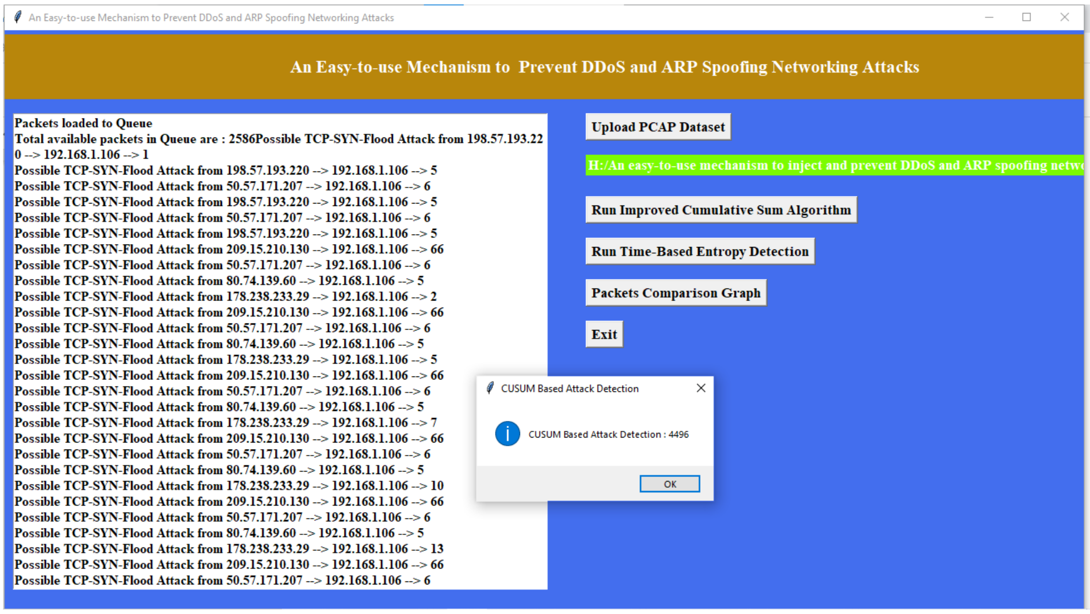
```
Packets loaded to Queue
Total available packets in Queue are : 2586Possible TCP-SYN-Flood Attack from 198.57.193.22
0 --> 192.168.1.106 --> 1
Possible TCP-SYN-Flood Attack from 198.57.193.220 --> 192.168.1.106 --> 5
Possible TCP-SYN-Flood Attack from 50.57.171.207 --> 192.168.1.106 --> 6
Possible TCP-SYN-Flood Attack from 198.57.193.220 --> 192.168.1.106 --> 5
Possible TCP-SYN-Flood Attack from 50.57.171.207 --> 192.168.1.106 --> 6
Possible TCP-SYN-Flood Attack from 198.57.193.220 --> 192.168.1.106 --> 5
Possible TCP-SYN-Flood Attack from 209.15.210.130 --> 192.168.1.106 --> 66
Possible TCP-SYN-Flood Attack from 50.57.171.207 --> 192.168.1.106 --> 6
Possible TCP-SYN-Flood Attack from 80.74.139.60 --> 192.168.1.106 --> 5
Possible TCP-SYN-Flood Attack from 178.238.233.29 --> 192.168.1.106 --> 2
Possible TCP-SYN-Flood Attack from 209.15.210.130 --> 192.168.1.106 --> 66
Possible TCP-SYN-Flood Attack from 50.57.171.207 --> 192.168.1.106 --> 6
Possible TCP-SYN-Flood Attack from 80.74.139.60 --> 192.168.1.106 --> 5
Possible TCP-SYN-Flood Attack from 178.238.233.29 --> 192.168.1.106 --> 5
Possible TCP-SYN-Flood Attack from 209.15.210.130 --> 192.168.1.106 --> 66
Possible TCP-SYN-Flood Attack from 50.57.171.207 --> 192.168.1.106 --> 6
Possible TCP-SYN-Flood Attack from 80.74.139.60 --> 192.168.1.106 --> 5
Possible TCP-SYN-Flood Attack from 178.238.233.29 --> 192.168.1.106 --> 7
Possible TCP-SYN-Flood Attack from 209.15.210.130 --> 192.168.1.106 --> 66
Possible TCP-SYN-Flood Attack from 50.57.171.207 --> 192.168.1.106 --> 6
Possible TCP-SYN-Flood Attack from 80.74.139.60 --> 192.168.1.106 --> 5
Possible TCP-SYN-Flood Attack from 178.238.233.29 --> 192.168.1.106 --> 10
Possible TCP-SYN-Flood Attack from 209.15.210.130 --> 192.168.1.106 --> 66
Possible TCP-SYN-Flood Attack from 50.57.171.207 --> 192.168.1.106 --> 6
Possible TCP-SYN-Flood Attack from 80.74.139.60 --> 192.168.1.106 --> 5
Possible TCP-SYN-Flood Attack from 178.238.233.29 --> 192.168.1.106 --> 13
Possible TCP-SYN-Flood Attack from 209.15.210.130 --> 192.168.1.106 --> 66
Possible TCP-SYN-Flood Attack from 50.57.171.207 --> 192.168.1.106 --> 6
```

Each packet is examined on the screen above, and the source and destination ports are shown. The CUSUM values for each packet are shown in the screen below.


Select C:\Windows\system32\cmd.exe
Activate Windows
Go to Settings to activate Windows.

```
CUSUM with attack : [ 8  9 10 11 12]
CUSUM with attack : [ 6  7  8  9 10]
CUSUM without attack : [4 5 6 7 8]
end Normal traffic from 176.62.165.177 --> 192.168.1.106 --> 105

CUSUM with attack : [ 9 10 11 12 13]
CUSUM without attack : [5 6 7 8 9]
end Normal traffic from 80.74.139.60 --> 192.168.1.106 --> 128

CUSUM with attack : [ 7  8  9 10 11]
CUSUM with attack : [ 7  8  9 10 11]
CUSUM without attack : [4 5 6 7 8]
end Normal traffic from 198.57.193.220 --> 192.168.1.106 --> 128

CUSUM with attack : [ 7  8  9 10 11]
CUSUM with attack : [ 7  8  9 10 11]
CUSUM without attack : [4 5 6 7 8]
end Normal traffic from 207.150.212.69 --> 192.168.1.106 --> 105

CUSUM with attack : [ 8  9 10 11 12]
CUSUM with attack : [ 6  7  8  9 10]
CUSUM without attack : [4 5 6 7 8]
end Normal traffic from 176.62.165.177 --> 192.168.1.106 --> 128

CUSUM with attack : [ 9 10 11 12 13]
CUSUM without attack : [5 6 7 8 9]
end Normal traffic from 80.74.139.60 --> 192.168.1.106 --> 105

CUSUM with attack : [ 7  8  9 10 11]
CUSUM with attack : [ 7  8  9 10 11]
CUSUM without attack : [4 5 6 7 8]
end Normal traffic from 198.57.193.220 --> 192.168.1.106 --> 105

CUSUM with attack : [ 7  8  9 10 11]
CUSUM with attack : [ 7  8  9 10 11]
CUSUM without attack : [4 5 6 7 8]
end Normal traffic from 207.150.212.69 --> 192.168.1.106 --> 128

CUSUM with attack : [ 8  9 10 11 12]
CUSUM with attack : [ 6  7  8  9 10]
CUSUM without attack : [4 5 6 7 8]
end Normal traffic from 176.62.165.177 --> 192.168.1.106 --> 128

CUSUM with attack : [ 9 10 11 12 13]
```

On the screen above, we can see that each packet has a CUSUM array, and we can see that when the CUSUM array has less values than when it has more values, there is no attack. On the screen above, the CUSUM value is [4 5 6 7 8] when there is no attack, and [7 8 9 10 11] when there is an assault. So we can determine if the request is a legitimate one or an attack by looking at this CUSUM array.

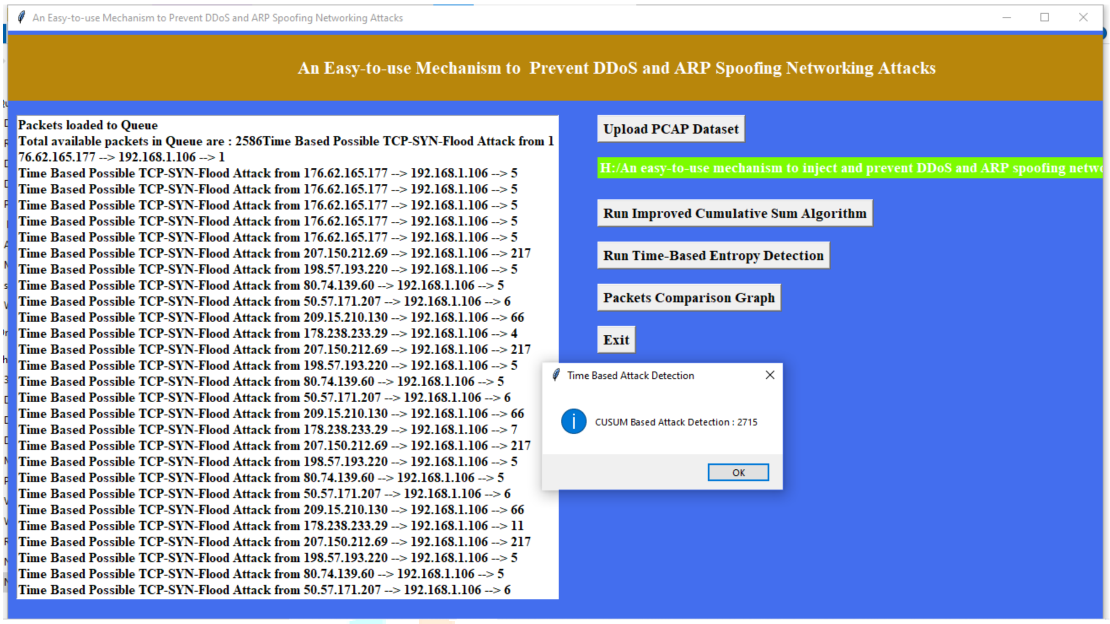

An Easy-to-use Mechanism to Prevent DDoS and ARP Spoofing Networking Attacks
An Easy-to-use Mechanism to Prevent DDoS and ARP Spoofing Networking Attacks
Upload PCAP Dataset
Run Improved Cumulative Sum Algorithm
Run Time-Based Entropy Detection
Packets Comparison Graph
Exit
CUSUM Based Attack Detection
OK

H:/An easy-to-use mechanism to inject and prevent DDoS and ARP spoofing netw

CUSUM Based Attack Detection : 4496

```
Packets loaded to Queue
Total available packets in Queue are : 2586Possible TCP-SYN-Flood Attack from 198.57.193.22
0 --> 192.168.1.106 --> 1
Possible TCP-SYN-Flood Attack from 198.57.193.220 --> 192.168.1.106 --> 5
Possible TCP-SYN-Flood Attack from 50.57.171.207 --> 192.168.1.106 --> 6
Possible TCP-SYN-Flood Attack from 198.57.193.220 --> 192.168.1.106 --> 5
Possible TCP-SYN-Flood Attack from 50.57.171.207 --> 192.168.1.106 --> 6
Possible TCP-SYN-Flood Attack from 198.57.193.220 --> 192.168.1.106 --> 5
Possible TCP-SYN-Flood Attack from 209.15.210.130 --> 192.168.1.106 --> 66
Possible TCP-SYN-Flood Attack from 50.57.171.207 --> 192.168.1.106 --> 6
Possible TCP-SYN-Flood Attack from 80.74.139.60 --> 192.168.1.106 --> 5
Possible TCP-SYN-Flood Attack from 178.238.233.29 --> 192.168.1.106 --> 2
Possible TCP-SYN-Flood Attack from 209.15.210.130 --> 192.168.1.106 --> 66
Possible TCP-SYN-Flood Attack from 50.57.171.207 --> 192.168.1.106 --> 6
Possible TCP-SYN-Flood Attack from 80.74.139.60 --> 192.168.1.106 --> 5
Possible TCP-SYN-Flood Attack from 178.238.233.29 --> 192.168.1.106 --> 5
Possible TCP-SYN-Flood Attack from 209.15.210.130 --> 192.168.1.106 --> 66
Possible TCP-SYN-Flood Attack from 50.57.171.207 --> 192.168.1.106 --> 6
Possible TCP-SYN-Flood Attack from 80.74.139.60 --> 192.168.1.106 --> 5
Possible TCP-SYN-Flood Attack from 178.238.233.29 --> 192.168.1.106 --> 7
Possible TCP-SYN-Flood Attack from 209.15.210.130 --> 192.168.1.106 --> 66
Possible TCP-SYN-Flood Attack from 50.57.171.207 --> 192.168.1.106 --> 6
Possible TCP-SYN-Flood Attack from 80.74.139.60 --> 192.168.1.106 --> 5
Possible TCP-SYN-Flood Attack from 178.238.233.29 --> 192.168.1.106 --> 10
Possible TCP-SYN-Flood Attack from 209.15.210.130 --> 192.168.1.106 --> 66
Possible TCP-SYN-Flood Attack from 50.57.171.207 --> 192.168.1.106 --> 6
Possible TCP-SYN-Flood Attack from 80.74.139.60 --> 192.168.1.106 --> 5
Possible TCP-SYN-Flood Attack from 178.238.233.29 --> 192.168.1.106 --> 13
Possible TCP-SYN-Flood Attack from 209.15.210.130 --> 192.168.1.106 --> 66
Possible TCP-SYN-Flood Attack from 50.57.171.207 --> 192.168.1.106 --> 6
```

As seen in the screenshot above, there are a total of 4496 assaults in the PCAP file. Now, to launch the Time Based method, click the "Run Time-Based Entropy Detection" button.

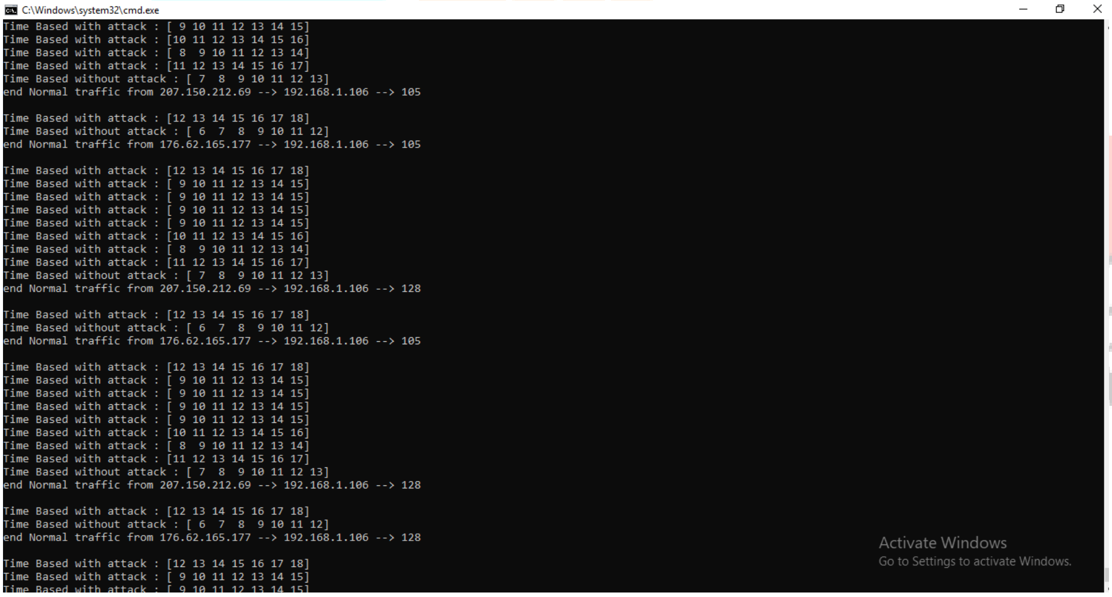

An Easy-to-use Mechanism to Prevent DDoS and ARP Spoofing Networking Attacks
An Easy-to-use Mechanism to Prevent DDoS and ARP Spoofing Networking Attacks
Upload PCAP Dataset
Run Improved Cumulative Sum Algorithm
Run Time-Based Entropy Detection
Packets Comparison Graph
Exit
Time Based Attack Detection
OK

H:/An easy-to-use mechanism to inject and prevent DDoS and ARP spoofing netw

CUSUM Based Attack Detection : 2715

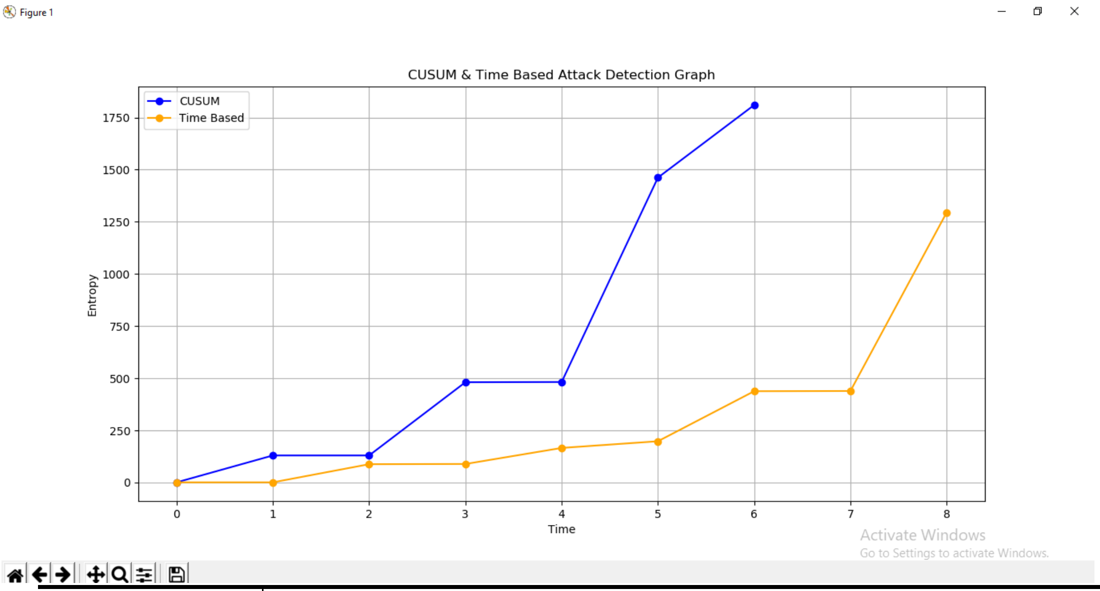
```
Packets loaded to Queue
Total available packets in Queue are : 2586Time Based Possible TCP-SYN-Flood Attack from 1
76.62.165.177 --> 192.168.1.106 --> 1
Time Based Possible TCP-SYN-Flood Attack from 176.62.165.177 --> 192.168.1.106 --> 5
Time Based Possible TCP-SYN-Flood Attack from 176.62.165.177 --> 192.168.1.106 --> 5
Time Based Possible TCP-SYN-Flood Attack from 176.62.165.177 --> 192.168.1.106 --> 5
Time Based Possible TCP-SYN-Flood Attack from 176.62.165.177 --> 192.168.1.106 --> 5
Time Based Possible TCP-SYN-Flood Attack from 176.62.165.177 --> 192.168.1.106 --> 5
Time Based Possible TCP-SYN-Flood Attack from 207.150.212.69 --> 192.168.1.106 --> 217
Time Based Possible TCP-SYN-Flood Attack from 198.57.193.220 --> 192.168.1.106 --> 5
Time Based Possible TCP-SYN-Flood Attack from 80.74.139.60 --> 192.168.1.106 --> 5
Time Based Possible TCP-SYN-Flood Attack from 50.57.171.207 --> 192.168.1.106 --> 6
Time Based Possible TCP-SYN-Flood Attack from 209.15.210.130 --> 192.168.1.106 --> 66
Time Based Possible TCP-SYN-Flood Attack from 178.238.233.29 --> 192.168.1.106 --> 4
Time Based Possible TCP-SYN-Flood Attack from 207.150.212.69 --> 192.168.1.106 --> 217
Time Based Possible TCP-SYN-Flood Attack from 198.57.193.220 --> 192.168.1.106 --> 5
Time Based Possible TCP-SYN-Flood Attack from 80.74.139.60 --> 192.168.1.106 --> 5
Time Based Possible TCP-SYN-Flood Attack from 50.57.171.207 --> 192.168.1.106 --> 6
Time Based Possible TCP-SYN-Flood Attack from 209.15.210.130 --> 192.168.1.106 --> 66
Time Based Possible TCP-SYN-Flood Attack from 178.238.233.29 --> 192.168.1.106 --> 7
Time Based Possible TCP-SYN-Flood Attack from 207.150.212.69 --> 192.168.1.106 --> 217
Time Based Possible TCP-SYN-Flood Attack from 198.57.193.220 --> 192.168.1.106 --> 5
Time Based Possible TCP-SYN-Flood Attack from 80.74.139.60 --> 192.168.1.106 --> 5
Time Based Possible TCP-SYN-Flood Attack from 50.57.171.207 --> 192.168.1.106 --> 6
Time Based Possible TCP-SYN-Flood Attack from 209.15.210.130 --> 192.168.1.106 --> 66
Time Based Possible TCP-SYN-Flood Attack from 178.238.233.29 --> 192.168.1.106 --> 11
Time Based Possible TCP-SYN-Flood Attack from 207.150.212.69 --> 192.168.1.106 --> 217
Time Based Possible TCP-SYN-Flood Attack from 198.57.193.220 --> 192.168.1.106 --> 5
Time Based Possible TCP-SYN-Flood Attack from 80.74.139.60 --> 192.168.1.106 --> 5
Time Based Possible TCP-SYN-Flood Attack from 50.57.171.207 --> 192.168.1.106 --> 6
```

As this method only monitors once every 10 seconds, the time-based programme identified 2715 assaults, resulting in a lower detection rate. In the black console below, we can observe Time Based CUSUM statistics.


C:\Windows\system32\cmd.exe
Activate Windows
Go to Settings to activate Windows.

```
Time Based with attack : [ 9 10 11 12 13 14 15]
Time Based with attack : [10 11 12 13 14 15 16]
Time Based with attack : [ 8  9 10 11 12 13 14]
Time Based with attack : [11 12 13 14 15 16 17]
Time Based without attack : [ 7  8  9 10 11 12 13]
end Normal traffic from 207.150.212.69 --> 192.168.1.106 --> 105

Time Based with attack : [12 13 14 15 16 17 18]
Time Based without attack : [ 6  7  8  9 10 11 12]
end Normal traffic from 176.62.165.177 --> 192.168.1.106 --> 105

Time Based with attack : [12 13 14 15 16 17 18]
Time Based with attack : [ 9 10 11 12 13 14 15]
Time Based with attack : [ 9 10 11 12 13 14 15]
Time Based with attack : [ 9 10 11 12 13 14 15]
Time Based with attack : [ 9 10 11 12 13 14 15]
Time Based with attack : [10 11 12 13 14 15 16]
Time Based with attack : [ 8  9 10 11 12 13 14]
Time Based with attack : [11 12 13 14 15 16 17]
Time Based without attack : [ 7  8  9 10 11 12 13]
end Normal traffic from 207.150.212.69 --> 192.168.1.106 --> 128

Time Based with attack : [12 13 14 15 16 17 18]
Time Based without attack : [ 6  7  8  9 10 11 12]
end Normal traffic from 176.62.165.177 --> 192.168.1.106 --> 105

Time Based with attack : [12 13 14 15 16 17 18]
Time Based with attack : [ 9 10 11 12 13 14 15]
Time Based with attack : [ 9 10 11 12 13 14 15]
Time Based with attack : [ 9 10 11 12 13 14 15]
Time Based with attack : [ 9 10 11 12 13 14 15]
Time Based with attack : [10 11 12 13 14 15 16]
Time Based with attack : [ 8  9 10 11 12 13 14]
Time Based with attack : [11 12 13 14 15 16 17]
Time Based without attack : [ 7  8  9 10 11 12 13]
end Normal traffic from 207.150.212.69 --> 192.168.1.106 --> 128

Time Based with attack : [12 13 14 15 16 17 18]
Time Based without attack : [ 6  7  8  9 10 11 12]
end Normal traffic from 176.62.165.177 --> 192.168.1.106 --> 128

Time Based with attack : [12 13 14 15 16 17 18]
Time Based with attack : [ 9 10 11 12 13 14 15]
Time Based with attack : [ 9 10 11 12 13 14 15]
```

In the previous screen, which is time-based, we can see more variation in requests in an attack scenario compared to a normal scenario. Click the "Packets Comparison Graph" button to access the graph below.



In the graph above, the x-axis shows time, the y-axis entropy values, and the blue line represents window-based CUSUM while the orange line represents time-based CUSUM. In both cases, we can observe that entropy values increased significantly when the attack took place. Up to 5 seconds on the x-axis of the following graph, both techniques have low entropy values. However, as the programme got more requests from the same IP, the entropy value increased.

TEST CASES:

S.NO	INPUT	If available	If not available
1	Upload PCAP dataset	Dataset loaded	There is no process
2	Run improved cumulative sum (CUSUM) algorithm	analyze pcap file with CUSUM technique	We can’t analyze
3	Run time based entropy detection	technique monitors once in 10 seconds	We cant run
4	Packets comparison graph	Entropy values displayed	We can't get graph

5. CONCLUSION & FUTURE SCOPE

This project demonstrated an instructional programme that automates the execution of SYN flood, ARP spoofing, and Ping flood attacks. Three current applications—packet, nemesis, and perf—were thoroughly examined. Then, to create and inject packets related to known attacks, a Python programme with a scapy library was created. This program's ease of use through the command line and the ability to automate an assault to hit several victims defined by their IP addresses must be highlighted. Three further essential incorporated features are the defining of an attacker's source IP address, the maximum number of packets to be transmitted, and the payload. The tests were carried out successfully on a fictitious network with a single attacker and two targets. The three implemented attacks were tested successfully, and all of the application's features were investigated. The programme has the capacity to expand, and it would be doable to include new features like the creation of various types of assaults as well as the integration of log files and statistics. The ability to launch an ARP spoofing attack concurrently on several targets across various networks while reading a text file with the victims' gateway IP addresses is a capability that will soon be available.

6. REFERENCES

[1] J. Mirkovic, and P. Reiher. "A DDoS attack and defensive mechanism taxonomy." Computer Communication Review, 34(2), ACM SIGCOMM, pp. 39-53, 2004.

[2] “Packit-network injection and capture”. [Online]. Available: http://packetfactory.openwall.net/projects/packit/.

[3] J. Nathan. “Packet injection tool suite”. [Online]. Available: http://nemesis.sourceforge.net/.

[4] “Pierf packet generator and analyzer”. [Online]. Available: http://pierf.sourceforge.net/.

[5] Philippe Biondi and the Scapy community. “Scapy”. [Online]. Available: https://scapy.net/.

[6] SecureAuthCorp. “Secureauthcorp/impacket”. [Online]. Available: https://github.com/SecureAuthCorp/impacket.

[7] M. Bogdanoski, T. Suminoski, and A. Risteski. “Analysis of the SYN flood DoS attack.” International Journal of Computer Network and Information Security (IJCNIS), 5(8), pp. 1-11, 2013.

[8] A. M. AbdelSalam, A. B. El-Sisi, and V. Reddy. “Mitigating ARP spoofing attacks in software-defined networks”. ICCTA 2015, Alexandria, Egypt, 2015.

[9] H. Harshita. “Detection and prevention of ICMP flood DDOS attack”. International Journal of New Technology and Research, 3(3), 263333, 2017.