MALWARE DETECTION IN NETWORK PACKETS

PR Project

TEAM MEMBERS

MENTOR
Dr. Vijaypal Singh Rathor

HIMANSHI ARORA
22BCS106

DAKSHATA BORSE
22BCS072

HIMANSHU
22BCS107

KARAN AGGARWAL
22BCS130

ISHAAN SONI
22BCS109

PROJECT INTRODUCTION

This project is designed to detect Distributed Denial of Service (DDoS) attacks within the same network interface. It monitors network traffic in real-time to identify and respond to suspicious activities originating from various IP addresses connected to the network. By leveraging advanced machine learning techniques, the system ensures proactive protection against potential DDoS attacks, safeguarding the integrity and availability of network resources.

PROJECT PHASES

Learning

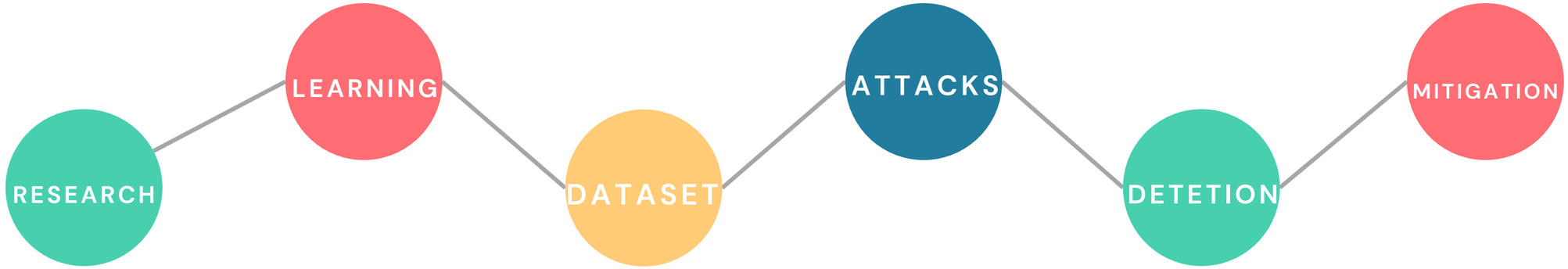
We explored various machine learning algorithms to understand their potential application in anomaly detection.

Understanding Attacks

We studied DoS and DDoS attacks in depth and learned how to simulate these attacks for testing purposes

Mitigation

iWe developed a system to block IP addresses identified as sources of DDoS attacks to stop ongoing attacks



Research Papers

We began by thoroughly reading research papers on DDoS attacks and network security.

Database Preparation

We prepared our original dataset files by sniffing network packets to collect real-time data

Detection

We implemented detection mechanisms using K-Means clustering and Random Forest classification to identify potential DDoS attacks

RESEARCH PAPER WE REFER

DENIAL OF SERVICE ATTACK DETECT IN DETECTION AND MITIGATION FOR INTERNET OF THINGS USING LOOKING-BACK-ENABLED MACHINE LEARNING TECHNIQUES

Computers and Electrical Engineering 98 (2022) 107716

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Denial of service attack detection and mitigation for internet of things using looking-back-enabled machine learning techniques☆

Alaeddine Mihoub [a], Ouissem Ben Fredj [b], Omar Cheikhrouhou [c,f,*], Abdelouahid Derhab [d], Moez Krichen [e]

[a] Department of Management Information Systems and Production Management, College of Business and Economics, Qassim University, P.O. Box: 6640, Buraidah: 51452, Saudi Arabia
[b] Higher Institute of Applied Sciences and Technology of Kairouan, University of Kairouan, Tunisia
[c] Higher Institute of Computer Science of Mahdia, University of Monastir, Mahdia 5111, Tunisia
[d] Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh 11653, Saudi Arabia
[e] Faculty of CSIT, Al-Baha University, Saudi Arabia, & ReDCAD Laboratory, University of Sfax, Tunisia
[f] CES Laboratory, National School of Engineers of Sfax, University of Sfax, Sfax 3038, Tunisia

ARTICLE INFO

Keywords:
Cybersecurity
DoS
DDoS
IoT
Machine Learning
Looking-Back method

ABSTRACT

IoT (Internet of Things) systems are still facing a great number of attacks due to their integration in several areas of life. The most-reported attacks against IoT systems are "Denial of Service" (DoS) and "Distributed Denial of Service" (DDoS) attacks. In this paper, we investigate DoS/DDoS attacks detection for IoT using machine learning techniques. We propose a new architecture composed of two components: DoS/DDoS detection and DoS/DDoS mitigation. The detection component provides fine-granularity detection, as it identifies the specific type of attack, and the packet type used in the attack. In this way, it is possible to apply the corresponding mitigation countermeasure on specific packet types. The proposed DoS/DDoS detection component is a multi-class classifier that adopts the "Looking-Back" concept, and is evaluated on the Bot-IoT dataset. Evaluation results show promising results as a Looking-Back-enabled Random Forest classifier achieves an accuracy of 99.81%.

1. Introduction

Internet of Things (IoT) is still emerging as a promising technology and it is more integrated with our daily life applications including smart transportation [1], smart healthcare [2], smart home [3], etc. The installed IoT devices worldwide are projected to reach 30.9 billion units by 2025 [4]. These IoT devices do not possess high computation power and do not have appropriate security mechanisms while they are connected to the Internet. This vast integration of IoT technology has made them an interesting target of attackers [5]. Two of the most challenging attacks in IoT are (1) Denial of Service (DoS) and (2) Distributed Denial of Service (DDoS). The problem is how to detect DoS/DDoS attacks, which are characterized by a high packet rate from one IP (for DoS) or multiple IPs (for DDoS), while normal traffic could also encompass a high traffic rate especially from environments equipped with IoT sensors. Cyber-attacks are considered as an obstacle to the spread of IoT devices. Therefore, the need for anomaly detection methods is of high

☆ This paper is for special section VSI-spc. Reviews were processed by Guest Editor Dr. Atilla Elci and recommended for publication.

* Corresponding author.
E-mail address: omar.cheikhrouhou@isetsf.rnu.tn (O. Cheikhrouhou).

https://doi.org/10.1016/j.compeleceng.2022.107716
Received 2 June 2021; Received in revised form 13 December 2021; Accepted 7 January 2022
Available online 18 January 2022
0045-7906/© 2022 Elsevier Ltd. All rights reserved.

PACKET SNIFFING AND SNIFFING DETECTION

International Journal of Innovations in Engineering and Technology (IJIET)
http://dx.doi.org/10.21172/ijiet.161.04

Packet Sniffing and Sniffing Detection

Ruchi Tuli
Department of Computer Science & Engineering, Jubail University College, Jubail, Kingdom of Saudi Arabia

Abstract - Packet sniffing is a process of monitoring and capturing all data packets passing thorough a given network using a software application or a hardware device. Sniffers can be used to monitor all sorts of traffic either protected or unprotected. Using sniffers, attacker can gain information which might be helpful for further attacks. This paper discusses the basic workingof a packet sniffer, network protocols that are vulnerable to sniffing, various software that can be used for sniffing. This paper also describes possible defensive techniques used to defend against sniffing attacks. Finally the papers ends with describing some sniffing detection techniques. Sniffers are not hacking tools but they can help a hacker to launch further attacks such as session hijacking, DOS attacks, MITM attacks etc.

Keywords - Wireshark, packet sniffing, network security, HTTP, FTP

I. Introduction

A sniffer is a program or a device that eavesdrops on the network traffic by grabbing information travelling over a network. Sniffers basically are "Data Interception" technology[1]. They work because Ethernet was built around a principle of sharing. Most networks use broadcast technology wherein messages for one computer can be read by another computer on that network. In practice, all the other computers except the one for which the message is meant, will ignore that message. However, computers can be made to accept messages even if they are not meant for them. This is done by means of a sniffer[1].

Using sniffing, the attacker can capture packets like Syslog traffic, DNS traffic, web traffic, Email and other types of data traffic. By capturing these packets, an attacker can reveal information such as data, username and passwords from protocols such as HTTP, POP, IMAP, SMTP, FTP and Telnet. The process of sniffing is performed by using Promiscuous ports. This paper discusses basic working of a packet sniffer, protocols that are vulnerable to sniffing, various types of tools used for sniffing, defensive techniques to defend against sniffing attacks and sniffing detection techniques[2].

II. Working of Sniffers

In the process of sniffing, an attacker gets connected to the target network to sniff the packets. Using sniffers, which turns Network Interface Card (NIC) of the attacker's system into promiscuous mode, attacker captures the packet[3]. Once attacker captures the packet, it can decrypt these packets to extract the information. Sniffers can use used to hack a system or a network. The steps that an attacker follows to make use of sniffers to hack a network are listedbelow and shown in Figure 1:

a) An attacker who decides to hack a network first discovers the appropriate switch to access the network and connects a system to one of the ports on the switch.
b) After succeeding in connecting to the switch, attacker tries to determine network information such as network topology by using network discovery tools.
c) By analyzing the network topology, the attacker identifies the victim's machine to target the attacks.
d) After target identification, the attacker uses ARP spoofing techniques to send a fake (spoofed) ARP message
e) The previous step helps the attacker to divert all the traffic from the victim's computer to the attacker's computer. This is a man-in-the-middle (MITM) attack.
f) Now the attacker can see all the data packets sent and received by the victim and can extract the confidential information such as username, password, credit card details, PIN etc.

PREDICT AND PREVENT DDOS ATTACKS USING MACHINE LEARNING AND STATISTICAL ALGORITHMS

Predict And Prevent DDOS Attacks Using Machine Learning and Statistical Algorithms

Azadeh Golduzian[1]

[1]Department of Mathematics and Statistics, University of New Mexico, NM 87106 USA

Corresponding author: Azadeh Golduzian (agolduzian96@unm.edu).

This work was supported in part by the University of New Mexico, Albuquerque.

A malicious attempt to exhaust a victim's resources to cause it to crash or halt its services is known as a distributed denial-of-service (DDoS) attack. DDOS attacks stop authorized users from accessing specific services available on the Internet. It targets varying components of a network layer and it is better to stop into layer 4 (transport layer) of the network before approaching a higher layer. This study uses several machine learning and statistical models to detect DDoS attacks from traces of traffic flow and suggests a method to prevent DDOS attacks. For this purpose, we used logistic regression, CNN, XGBoost, naive Bayes, AdaBoostClassifier, KNN, and random forest ML algorithms. In addition, data preprocessing was performed using three methods to identify the most relevant features. This paper explores the issue of improving the DDOS attack detection accuracy using the latest dataset named CICDDoS2019, which has over 50 million records. Because we employed an extensive dataset for this investigation, our findings are trustworthy and practical. Our target class (attack class) was imbalanced. Therefore, we used two techniques to deal with imbalanced data in machine learning. The XGboost machine learning model provided the best detection accuracy of (99.9999%) after applying the SMOTE approach to the target class, outperforming recently developed DDoS detection systems. To the best of our knowledge, no other research has worked on the most recent dataset with over 50 million records, addresses the statistical technique to select the most significant feature, has this high accuracy, and suggests ways to avoid DDOS attack

I. INTRODUCTION

The phenomenon known as a "Distributed Denial-of-Service (DDoS) Attack" constitutes a formidable form of cybercrime that unleashes havoc by inundating a server with an overwhelming barrage of requests, effectively rendering online sites and services inaccessible to legitimate users. The insidious intent behind a DDoS attack lies in its capacity to disrupt the seamless provision of both internal and external services offered by a website [1]. What sets DDoS attacks apart in their potency is their utilization of a multitude of compromised computer systems as sources for the deluge of attack traffic. This assortment of exploited machines extends to encompass a gamut of devices, including computers and networked resources such as Internet of Things (IoT) devices [1]. The advent of the Internet of Things (IoT) heralds an interconnected realm wherein objects interlink to glean and exchange information autonomously, erasing the need for manual intervention [2]. However, as the IoT's omnipresence burgeons, the proliferation of remote employees and the surge in Internet-connected devices come with a caveat. IoT devices, while prolific, may not consistently uphold robust security measures, leaving the networks they permeate susceptible to infiltration and malicious attacks.

Hence, the imperativeness of DDoS prediction and fortification looms large. An intriguing dichotomy emerges when inspecting DDoS attack trends; the frequency of such attacks witnessed a discernible dip from the onset of 2021 until its culmination, while maintaining relative consistency over the preceding biennium. Remarkably, 2021 exhibited a mere 3% reduction compared to the prior year. Paradoxically, as the attack frequency wanes, the magnitude of these attacks experiences exponential growth [3]. Envision a malevolent hacker striving to incapacitate a service. Here, the hacker's modus operandi veers from employing a solitary computer and static IP address; instead, an arsenal of diverse computers, each equipped with distinct IP addresses, is wielded to elude security measures. A pivotal hallmark of DDOS attacks is their orchestrated orchestration from a multitude of hosts, encompassing even the manipulation of your server to assail another. Often orchestrated by botnets, these attacks unfold through networks of automated robots or computers, each programmed to execute specific tasks—a landscape where the term "zombies" finds relevance. Historically, the roots of DDoS trace back to 1998, though the full impact remained obscure until July 1999, when influential organizations and corporate entities endured the brunt of these assaults [4]. The repercussions of such attacks are far-reaching, with organizations and communications infrastructures susceptible to debilitating disruptions that may extend to minutes or even hours, if proactive protection mechanisms are not in place. Thus, the urgency to fortify digital bastions against these evolving threats has never been more critical.

LEARNING ML ALGORITHMS

ALGO USED

- .K-Means Clustering: for unsupervised anomaly detection.
- Random Forest: for classification and detecting anomalies.
- Isolation Forest: for identifying outliers in the data.
- Support Vector Machines (SVM): for binary classification tasks.

DATABASE PREPARATION

WE PREPARED OUR ORIGINAL DATASET FILES BY SNIFFING NETWORK PACKETS TO COLLECT REAL-TIME DATA

```
,TPC,TPL,APL,PLV,ALD,TPT,APT,ATD,PTV,Rate
192.168.31.179,60,21087,526.03125,279798.7802734375,308.83870967741933,10331.940047398535,0.17219899866046726,1.9094664973597373,460.9472265022596,3.05478692728754
142.250.194.206,27,2248,83.92307692307692,568.0710059171596,19.28,4649.37293767616,0.1721989975179994,2.367986717224121,290.56963280482796,0.48736100751286143
104.18.13.201,2,132,66.0,0.0,0.0,344.39799847654865,0.17219899923827434,0.0004162788391113281,4.332201797296875e-08,0.38327748878885654
0.0.0.0,3,1116,372.0,8.0,3.0,516.5969994437513,0.17219899981458378,1.0072503089904785,0.8954736525809986,2.1602912932162965
192.168.31.1,8,2309,335.25,3621.1875,112.33333333333333,1377.5920163291362,0.1721990010331479,7.6184306144714355,128.7315254183396,1.9468754057142597
104.46.162.227,3,198,66.0,0.0,0.0,516.5970054067408,0.17219900033446828,2.4497716426849365,1.5003452753258273,0.3832774863489674
185.125.190.18,4,461,115.25,6520.6875,128.66666666666666,688.796010348655,0.17219900258716375,0.13655718167622885,0.020978859591039623,0.6692837836947557
34.107.243.93,3,222,74.0,128.0,12.0,516.5970082185161,0.17219900273950536,0.010496139526367188,8.372348808431222e-05,0.42973535748022745
216.58.200.170,12,3902,325.1666666666667,158447.63888888888,362.72727272727275,2066.3880421279596,0.1721990035106633,0.03724889321760698,0.010167165755736582,1.8883
192.168.31.179,51,20597,474.3030303030303,304864.5748393023,331.28125,8782.149565563177,0.17219900974760025,1.2132596373558044,190.64401460330336,2.7543888376491674
142.250.194.206,3,276,85.5,380.25,39.0,516.5970301769854,0.17219900810723338,2.384185791015625e-07,2.842170943040401e-14,0.49651853944917407
104.46.162.227,16,1428,86.27272727272727,1486.5619834710744,48.2,2755.1841831565184,0.1721990108876114,3.2013479709625243,70.39820000883846,0.5010059397439549
192.168.31.1,6,1881,239.33333333333334,19362.88888888889,156.5,1033.194069265727,0.17219900869428637,2.6625354290008545,6.301417134121702,1.3898647567607891
142.250.77.206,19,7143,410.11764705882354,253519.7508650519,437.4375,3271.781174438965,0.17219900855908934,0.03841395676136017,0.031800782302204476,2.38164929339934
34.149.97.1,2,171,85.5,380.25,39.0,344.39802393576656,0.1721990119678833,0.0005636215209960938,7.941730473248754e-08,0.4965185283173782
192.168.31.244,4,884,221.0,17700.0,106.66666666666667,688.7960528980601,0.17219901322451503,2.770353396733602,11.667608903574518,1.2833987597353864
0.0.0.0,3,1116,372.0,8.0,3.0,516.5970413868248,0.17219901379560826,1.0048060417175293,0.8933300680933295,2.1602911178199062
142.250.193.34,2,171,85.5,380.25,39.0,344.39802780647034,0.17219901390323517,4.76837158203125e-07,5.684341886080802e-14,0.49651852273698577
192.168.31.179,92,11819,128.4673913043478,26592.66198015124,116.0989010989011,15842.309925640595,0.17219902093087602,0.7167444700723166,131.53137051952544,0.7460401
34.149.97.1,6,498,83.0,266.0,25.8,1033.1941190693424,0.17219901984489042,4.759668684005737,78.47883171137626,0.4820004206456163
142.250.194.206,2,132,66.0,0.0,0.0,344.3980391530278,0.1721990195765139,7.152557373046875e-07,1.4210854715202004e-13,0.3832774435203677
142.250.193.34,4,342,85.5,380.25,13.0,688.7960804999943,0.17219902012499858,1.5297250747680664,3.937136651631789,0.4965185047971579
192.168.31.1,8,1282,160.25,2121.1875,22.714285714285715,1377.5921634922206,0.17219902043652757,1.1329810278756278,11.770485573705166,0.930609242687696
142.250.77.206,3,237,79.0,338.0,39.0,516.5970607199162,0.17219902023997205,0.0026787519454956055,4.997758291362213e-06,0.4587714836583139
34.107.221.82,19,2008,105.6842105263158,8020.321329639887,81.55555555555556,3271.781405485672,0.17219902134135118,2.304621524280972,220.32938169779874,0.61373293357
34.107.243.93,2,160,80.0,196.0,28.0,344.3980405529332,0.1721990202764666,0.337200403213501,0.02842602798185112,0.464578717530213
13.107.13.93,45,22197,493.26666666666665,272817.08444444434,354.45454545454544,7748.955972139664,0.17219902160310363,0.3350924416021867,41.54186419494049,2.86451492
104.46.162.227,1,66,66.0,0.0,0.0,172.1990211141914,0.1721990211141914,0.0,0.0,0.38327744009783316
192.168.31.179,769,592517,770.5032509752926,376070.95480087475,206.80338541666666,132421.07999925807,0.17219906371815094,0.08926631075640519,275.6672476130993,4.474
34.107.221.82,16,1056,66.0,0.0,0.0,2755.1850326904955,0.17219906454315598,4.249042050043742,483.5779972534554,0.3832773434344604
```

UNDERSTANDING ATTACKS

DDOS ATTACKS

- UDP Flood: In this attack, the attacker sets up random ports on the target network by sending IP packets containing UDP datagrams.

- HTTP Flood: This attack uses several, seemingly genuine HTTP GET or POST requests to target an application or web server.

- Ping Flood and Ping of Death: Another typical flood attack exploits many ICMP echo queries.

- SYN Flood: Using an SYN flood, the attacker rapidly overwhelms the victim with connection requests

PERFORMING DDOS ATTACK

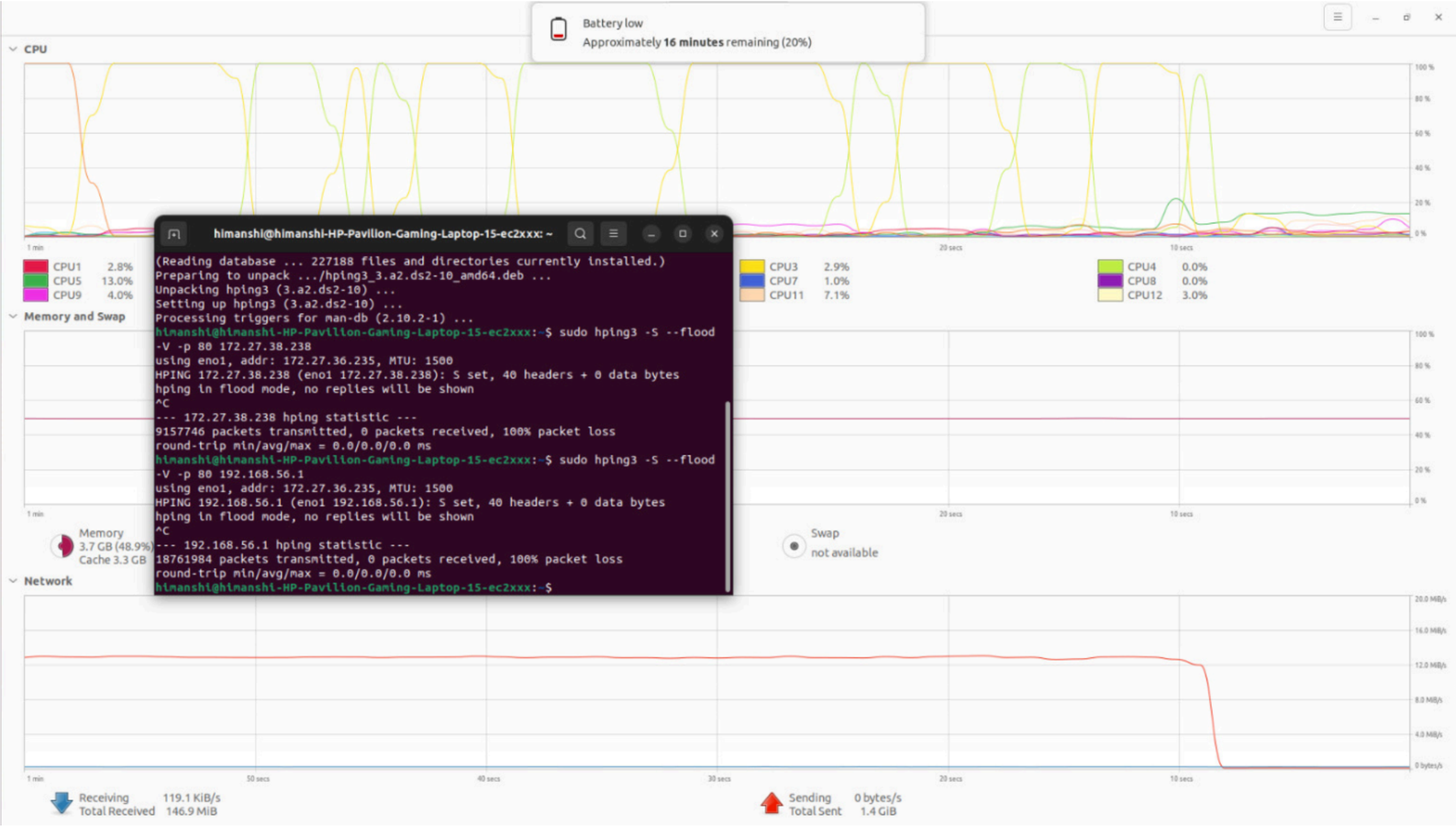
BEFORE ATTACK
SYSTEM MONITOR

BEFORE ATTACK
PACKETS SNIFFING

```
himanshi@himanshi-HP-Pavilion-Gaming-Laptop-15-ec2xxx:~/Documents/sh$ sudo python3 new.py
[sudo] password for himanshi:
/home/himanshi/Documents/sh/new.py:2: DeprecationWarning:
Pyarrow will become a required dependency of pandas in the next major release of pandas (pandas 3.0),
(to allow more performant data types, such as the Arrow string type, and better interoperability with other libraries)
but was not found to be installed on your system.
If this would cause problems for you,
please provide us feedback at https://github.com/pandas-dev/pandas/issues/54466

  import pandas as pd
^CAccumulating data...
                TPC    TPL       APL          PLV      ALD        TPT    APT    ATD      PTV   Rate
192.168.43.63     4    868   217.000        0.000    0.000    685.149  0.171  1.038    1.399  1.267
192.168.43.87   456  66553   145.950    47022.956  123.624  78106.988  0.171  0.127  115.321  0.852
51.132.193.104    6    499    83.167     1473.472   41.200   1027.724  0.171  9.441  300.675  0.486
192.168.43.1    150  24737   164.913     4148.119   68.403  25693.088  0.171  0.206   88.846  0.963
34.117.237.239   13   5961   458.538   265144.556  445.667   2226.734  0.171  0.111    0.246  2.677
34.107.221.82     8    752    94.000     5056.000   62.857   1370.298  0.171  7.401  360.052  0.549
34.149.100.209   74  54832   740.973   652225.783  495.068  12675.257  0.171  0.038    0.714  4.326
34.107.243.93    15   5908   393.867   483333.716  596.714   2569.309  0.171  0.133    0.327  2.299
34.120.208.123   43   9485   220.581   189952.383  212.333   7365.352  0.171  0.312   17.609  1.288
152.195.38.76     8   1272   159.000    59071.000  211.429   1370.298  0.171  7.343  352.932  0.928
34.120.115.102   23  26948  1171.652  1240129.792  772.091   3939.607  0.171  0.186    2.887  6.840
52.10.78.57      10   4059   405.900   370969.490  436.000   1712.873  0.171  0.173    0.327  2.370
44.239.14.124     9   3758   417.556   640380.025  652.750   1541.585  0.171  0.160    0.249  2.438
13.107.5.93       2    108    54.000        0.000    0.000    342.575  0.171  0.205    0.010  0.315
117.18.232.200    6    477    79.500      455.250   22.800   1027.724  0.171  2.847   44.457  0.464
108.159.46.115   22  15524   705.636   527295.322  519.905   3768.320  0.171  0.039    0.066  4.120
18.161.125.68    25  14094   563.760   539617.302  371.667   4282.181  0.171  0.013    0.007  3.291
108.159.47.187    6   1348   224.667   123358.222  379.200   1027.724  0.171  6.220  142.721  1.312
34.196.172.205   13   8361   643.154   774247.822  769.333   2226.734  0.171  0.066    0.048  3.755
13.107.6.175      1     54    54.000        0.000    0.000    171.287  0.171  0.000    0.000  0.315
35.201.103.21    11   5592   508.364   601194.050  797.800   1884.160  0.171  0.082    0.057  2.968
34.98.75.36      12   4803   400.250   570683.688  581.091   2055.447  0.171  0.093    0.099  2.337
Regression Results:
Slope: 0.05339356295878036
Intercept: 1.5375494071146245
R-value: 0.20991999442009393
P-value: 0.34842742731651843
Standard Error: 0.05560757558814648
```

AFTER ATTACK
SYSTEM MONITOR



AFTER ATTACK
PACKETS SNIFFING

```
  import pandas as pd
Accumulating data...
Accumulating data...
Accumulating data...
Accumulating data...
Accumulating data...
Accumulating data...
Accumulating data...
Accumulating data...
Accumulating data...
Accumulating data...
Accumulating data...
Accumulating data...
Accumulating data...
Accumulating data...
Accumulating data...
Accumulating data...
Accumulating data...
Accumulating data...
Accumulating data...
^CAccumulating data...
Accumulating data...
Accumulating data...
Accumulating data...
^CAccumulating data...
                   TPC     TPL      APL          PLV     ALD          TPT    APT    ATD    PTV   Rate
192.168.43.63   103719 6846172   66.000        0.000    0.00 1.776575e+07  0.171  0.001  1.541  0.385
192.168.43.87    98623 5327284   54.000        0.000    0.00 1.689287e+07  0.171  0.001  1.568  0.315
192.168.43.1         7     881  134.600     1072.240   62.75 1.199012e+03  0.171  0.020  0.001  0.786
117.18.232.200      10    7755  854.333  1060833.556  613.75 1.712873e+03  0.171  0.019  0.002  4.988
34.107.243.93        2     156   78.000      144.000   24.00 3.425750e+02  0.171  0.204  0.010  0.455
34.120.208.123       2     132   66.000        0.000    0.00 3.425750e+02  0.171  0.000  0.000  0.385
Regression Results:
Slope: 0.13205714285714287
Intercept: 0.8888571428571429
R-value: 0.13326243515226766
P-value: 0.8012896428437541
Standard Error: 0.4910584769201139
```

ATTACK DETECTION

DETECTION BY K-MEANS CLUSTERING

DETECTS ANOMALY

```
192.168.31.79     11   820   74.545455     156.429752   18.200000  1894.012384  0.172183  1.372179  1.781046e+01  0.432943        0
104.18.31.2        2   171   85.500000     380.250000   39.000000   344.365887  0.172183  0.000287  2.053190e-08  0.496565        1
192.168.31.1       2   282  141.000000      36.000000   12.000000   344.365888  0.172183  0.000111  3.099245e-09  0.818896        1
142.250.194.206   16  4285  267.812500  121693.652344  296.133333  2754.927104  0.172183  0.054647  3.938202e-02  1.555395        1
Potential anomaly detected from IP: 104.208.16.88
Potential anomaly detected from IP: 192.168.31.179
Potential anomaly detected from IP: 104.18.31.2
Potential anomaly detected from IP: 192.168.31.1
Potential anomaly detected from IP: 142.250.194.206
IP address that occurred most frequently: 192.168.31.179 (Count: 26)
^CAccumulating data...
                TPC   TPL        APL          PLV        ALD          TPT       APT       ATD           PTV      Rate  Cluster
104.208.16.88     8  5627  703.375000  291924.984375  392.714286  1377.463547  0.172183  0.085234  4.384654e-02  4.085045        1
192.168.31.179   26  6885  264.807692  162267.386095  311.320000  4476.756536  0.172183  0.274512  8.791713e+00  1.537944        1
192.168.31.79    43  7825   74.545455     156.429752   18.200000  7403.866663  0.172183  1.372179  1.781046e+01  0.432943        0
104.18.31.2       2   171   85.500000     380.250000   39.000000   344.365887  0.172183  0.000287  2.053190e-08  0.496565        1
192.168.31.1      2   282  141.000000      36.000000   12.000000   344.365888  0.172183  0.000111  3.099245e-09  0.818896        1
142.250.194.206  16  4285  267.812500  121693.652344  296.133333  2754.927104  0.172183  0.054647  3.938202e-02  1.555395        1
Potential anomaly detected from IP: 104.208.16.88
Potential anomaly detected from IP: 192.168.31.179
Potential anomaly detected from IP: 104.18.31.2
Potential anomaly detected from IP: 192.168.31.1
Potential anomaly detected from IP: 142.250.194.206
IP address that occurred most frequently: 192.168.31.79 (Count: 43)
^CAccumulating data...
                TPC    TPL        APL          PLV        ALD          TPT       APT       ATD           PTV      Rate  Cluster
104.208.16.88     8   5627  703.375000  291924.984375  392.714286  1377.463547  0.172183  0.085234  4.384654e-02  4.085045        1
192.168.31.179   43  13787  264.807692  162267.386095  311.320000  7403.866648  0.172183  0.274512  8.791713e+00  1.537944        1
192.168.31.79    73  12364   74.545455     156.429752   18.200000 12569.355091  0.172183  1.372179  1.781046e+01  0.432943        0
104.18.31.2       2    171   85.500000     380.250000   39.000000   344.365887  0.172183  0.000287  2.053190e-08  0.496565        1
192.168.31.1      4    890  141.000000      36.000000   12.000000   688.731783  0.172183  0.000111  3.099245e-09  0.818896        1
142.250.194.206  16   4285  267.812500  121693.652344  296.133333  2754.927104  0.172183  0.054647  3.938202e-02  1.555395        1
142.250.194.14   15   2764  184.266667   61160.995556  215.571429  2582.744217  0.172183  0.046678  2.883609e-02  1.070180        1
Potential anomaly detected from IP: 104.208.16.88
Potential anomaly detected from IP: 192.168.31.179
Potential anomaly detected from IP: 104.18.31.2
Potential anomaly detected from IP: 192.168.31.1
Potential anomaly detected from IP: 142.250.194.206
Potential anomaly detected from IP: 142.250.194.14
IP address that occurred most frequently: 192.168.31.79 (Count: 73)
^CAccumulating data...
                TPC    TPL        APL          PLV        ALD          TPT       APT           ATD           PTV      Rate  Cluster
104.208.16.88     8   5627  703.375000  291924.984375  392.714286  1377.463547  0.172183  8.523423e-02  4.384654e-02  4.085045        1
192.168.31.179   49  14300  264.807692  162267.386095  311.320000  8436.964345  0.172183  2.745125e-01  8.791713e+00  1.537944        1
192.168.31.79    85  13242   74.545455     156.429752   18.200000 14635.550490  0.172183  1.372179e+00  1.781046e+01  0.432943        0
104.18.31.2       3    276   85.500000     380.250000   39.000000   516.548837  0.172183  2.865791e-04  2.053190e-08  0.496565        1
192.168.31.1      4    890  141.000000      36.000000   12.000000   688.731783  0.172183  1.113415e-04  3.099245e-09  0.818896        1
142.250.194.206  18   4456  267.812500  121693.652344  296.133333  3099.293003  0.172183  5.464727e-02  3.938202e-02  1.555395        1
142.250.194.14   15   2764  184.266667   61160.995556  215.571429  2582.744217  0.172183  4.667786e-02  2.883609e-02  1.070180        1
34.117.188.166    2    171   85.500000     380.250000   39.000000   344.365898  0.172183  7.152557e-07  1.421085e-13  0.496565        1
Potential anomaly detected from IP: 104.208.16.88
Potential anomaly detected from IP: 192.168.31.179
Potential anomaly detected from IP: 104.18.31.2
Potential anomaly detected from IP: 192.168.31.1
Potential anomaly detected from IP: 142.250.194.206
Potential anomaly detected from IP: 142.250.194.14
Potential anomaly detected from IP: 34.117.188.166
IP address that occurred most frequently: 192.168.31.79 (Count: 85)
```

INTEGRATION OF THRESHOLD VALUE AND SYN-FIN CHECK

INTEGRATION OF THRESHOLD VALUE AND SYN-FIN CHECK

```
packet_counts[ip_src] += 1

# Remove packets that are outside the time window
while packet_times[ip_src] and packet_times[ip_src][0] < current_time - TIME_WINDOW:
    packet_times[ip_src].pop(0)
    packet_counts[ip_src] -= 1

# Alert if threshold is exceeded
if packet_counts[ip_src] > PACKET_THRESHOLD:
    print(f"Alert! Potential DDoS attack detected from {ip_src}.")
    block_ip(ip_src)  # Block the IP address
    packet_counts[ip_src] = 0

# Check for SYN-FIN packets
if TCP in packet and packet[TCP].flags == 0x03:
    print(f"Alert! SYN-FIN packet detected from {ip_src}.")
    block_ip(ip_src)  # Block the IP address
```

RESULT OF INTEGRATION

```
/home/himanshi/Documents/sh/jul3.py:2: DeprecationWarning:
Pyarrow will become a required dependency of pandas in the next major release of pandas (pandas 3.0),
(to allow more performant data types, such as the Arrow string type, and better interoperability with other libraries)
but was not found to be installed on your system.
If this would cause problems for you,
please provide us feedback at https://github.com/pandas-dev/pandas/issues/54466

  import pandas as pd
^CAlert! Potential DDoS attack detected from 192.168.31.179.
Accumulating data...
                  TPC     TPL         APL            PLV         ALD            TPT       APT        ATD          PTV      Rate  Anomaly
192.168.31.179   1133  375961  331.827891  227168.689708  289.909011  195099.295997  0.172197   0.147135  1897.493526  1.927024       -1
142.250.193.78      3     244   81.333333     470.222222   23.000000     516.591228  0.172197  13.420290   160.089992  0.472327        1
192.168.31.1       73   10467  143.383562    4973.989867   53.125000   12570.387379  0.172197   2.309234  2434.249245  0.832671        1
163.70.145.60      38    4708  123.894737    6884.462604   77.945946    6543.489355  0.172197   3.365275   800.436613  0.719494        1
142.251.12.84      58   21287  367.017241  231580.982461  362.035088    9987.430764  0.172197   1.843818  1760.668000  2.131379        1
142.250.193.46    133   41143  309.345865  192380.045791  273.977273   22902.212368  0.172197   1.061854  1656.690650  1.796464        1
142.250.195.3     120   60646  505.383333  295014.119722  189.798319   20663.650487  0.172197   1.113872   693.513293  2.934912        1
216.58.196.106      9     734   81.555556     271.802469   20.875000    1549.773714  0.172197   6.615513   598.360464  0.473618        1
185.125.190.48      4     461  115.250000    6520.687500  128.666667     688.788310  0.172197   0.506417     0.298996  0.669291        1
142.250.206.106    63   21093  334.809524  194660.249433  264.790323   10848.416033  0.172197   1.615744   666.494909  1.944339        1
140.82.113.26       2     169   84.500000     930.250000   61.000000     344.394156  0.172197   0.306573     0.023497  0.490717        1
34.107.243.93       4     328   82.000000     120.000000   17.333333     688.788327  0.172197  24.959955  1394.455056  0.476199        1
142.250.195.10      3     210   70.000000      32.000000    6.000000     516.591241  0.172197   0.616934     0.336156  0.406511        1
142.250.207.202     2     171   85.500000     380.250000   39.000000     344.394161  0.172197   0.813089     0.165278  0.496524        1
34.117.188.166      5     459   91.800000     275.760000   33.000000     860.985412  0.172197  12.900890   624.987642  0.533110        1
142.250.192.197    23    4529  196.913043   87252.514178  192.545455    3960.532989  0.172197   3.279517   570.779821  1.143533        1
172.217.167.238    36   18790  521.944444  336124.219136  505.914286    6199.094922  0.172197   1.397763   139.313618  3.031088        1
142.250.195.1      40   35063  876.575000  325010.094375  329.948718    6887.883398  0.172197   2.634232  2464.735047  5.090533        1
140.82.112.26     117   52738  450.752137  259354.203521  299.327586   20147.058718  0.172197   0.323112   207.714929  2.617653        1
142.250.194.138    37    6286  169.891892   45013.123448  163.833333    6371.292166  0.172197   2.948445  2597.824292  0.986613        1
142.250.194.99     18    3001  166.722222   61331.200617  193.529412    3099.547551  0.172197   3.491836   753.765258  0.968206        1
185.125.190.56      1      90   90.000000       0.000000    0.000000     172.197084  0.172197   0.000000     0.000000  0.522657        1
34.107.221.82      12    1240  103.333333    6392.888889   80.727273    2066.365047  0.172197   4.805790   338.912261  0.600088        1
140.82.114.25       9    4511  501.222222  275755.728395  352.000000    1549.773791  0.172197   0.084628     0.047902  2.910747        1
142.250.194.78      7    1343  191.857143   69136.693878  258.666667    1205.379634  0.172197   0.067280     0.011640  1.114172        1
209.85.226.7       27   12727  471.370370  287946.381344  287.384615    4649.321464  0.172197   0.124637     1.052666  2.737389        1
Potential anomaly detected from IP: 192.168.31.179
IP address with the most frequent anomalies: 192.168.31.179 (Count: 1)
himanshi@himanshi-HP-Pavilion-Gaming-Laptop-15-ec2xxx:~/Documents/sh$
```

INTEGRATION OF RANDOM FOREST CLASSIFICATION

```
  warnings.warn(
                TPC     TPL          APL           PLV         ALD           TPT       APT           ATD           PTV      Rate  Anomaly  Anomaly_RF
192.168.31.179  847  275735   325.543093  220836.401626  193.341608  145851.014972  0.172197  4.117396e-02  4.688951e+01  1.890525        1           0
142.250.193.46   21    3501   166.714286   50147.918367  167.600000    3616.140860  0.172197  1.520714e+00  8.841179e+01  0.968159        1           0
142.250.193.78    8     567    70.875000     202.359375   16.285714    1377.577461  0.172197  5.853244e-02  1.920364e-02  0.411592        1           0
142.250.206.131  31    5369   173.193548   45977.833507  176.566667    5338.112714  0.172197  1.082522e+00  1.906856e+02  1.005786        1           0
192.168.31.1     24    3910   162.916667    6099.993056   63.347826    4132.732408  0.172197  9.076541e-01  5.154687e+01  0.946105        1           0
172.217.166.197  21    4289   204.238095   87732.371882  204.800000    3616.140844  0.172197  3.427576e-01  7.416773e+00  1.186071        1           0
142.250.194.170   7     996   142.285714    4051.632653   53.666667    1205.380286  0.172197  5.033152e+00  1.459884e+02  0.826295        1           0
34.107.243.93     2     160    80.000000     196.000000   28.000000     344.394365  0.172197  3.637180e-01  3.307270e-02  0.464584        1           0
34.107.221.82    14    1886   134.714286   11628.346939   79.692308    2410.760569  0.172197  2.399041e+00  1.343818e+02  0.782326        1           0
104.18.31.2       4     288    72.000000      36.000000   12.000000     688.788730  0.172197  4.271642e-02  2.790865e-03  0.418125        1           0
140.82.112.26     2     160    80.000000     196.000000   28.000000     344.394365  0.172197  2.384186e-07  2.842171e-14  0.464584        1           0
216.58.200.174   56   12473   222.732143   86564.231824  212.654545    9643.042300  0.172197  2.045120e-01  1.960077e+01  1.293471        1           0
163.70.145.60    54   16830   311.666667  159607.370370  277.396226    9298.647930  0.172197  1.525566e-01  2.003907e+00  1.809941        1           0
142.250.194.182 453  599027  1322.355408   82085.897967   93.566372   78005.324492  0.172197  1.363645e-02  6.350573e+00  7.679309        1           0
142.250.182.174 241  196982   817.352697  947090.352783  252.458333   41499.521441  0.172197  7.252658e-02  1.625735e+01  4.746609        1           0
142.250.182.163   6    3854   642.333333  321618.222222  285.200000    1033.183104  0.172197  2.291961e-02  1.337828e-03  3.730220        1           0
142.250.195.1    31   25178   812.193548  330670.091571  431.833333    5338.112709  0.172197  1.693616e-01  2.927686e+00  4.716648        1           0
49.44.208.81   2144 2980347  1390.087220   10577.371590    6.861409  369190.763542  0.172197  2.392175e-03  3.957804e+00  8.072648       -1           0
142.250.195.22   23   18145   788.913043  359718.862004  475.500000    3960.535239  0.172197  1.120394e-02  4.121456e-03  4.581451        1           0
142.250.77.234   39   20985   538.076923  342501.045365  298.789474    6715.690189  0.172197  1.991017e-02  3.643847e-02  3.124772        1           0
142.250.207.194  21    8665   412.619048  266247.664399  196.750000    3616.140872  0.172197  2.139732e-02  2.322605e-02  2.396201        1           0
49.44.208.76    403  547597  1358.801489   43896.536276   28.942786   69395.465432  0.172197  1.548808e-02  2.758755e-01  7.890962        1           0
^CAccumulating data...
/usr/local/lib/python3.10/dist-packages/sklearn/base.py:493: UserWarning: X does not have valid feature names, but RandomForestClassifier was fitted with featu
  warnings.warn(
                TPC     TPL          APL           PLV         ALD           TPT       APT           ATD           PTV      Rate  Anomaly  Anomaly_RF
192.168.31.179 1836  682414   325.543093  2.208364e+05  193.341608  316154.035872  0.172197  4.117396e-02  4.688951e+01  1.890525        1           0
142.250.193.46   63    9999   166.714286  5.014792e+04  167.600000   10848.422811  0.172197  1.520714e+00  8.841179e+01  0.968159        1           0
142.250.193.78    8     567    70.875000  2.023594e+02   16.285714    1377.577461  0.172197  5.853244e-02  1.920364e-02  0.411592        1           0
142.250.206.131  65    9718   173.193548  4.597783e+04  176.566667   11192.817201  0.172197  1.082522e+00  1.906856e+02  1.005786        1           0
192.168.31.1     32    5003   162.916667  6.099993e+03   63.347826    5510.309926  0.172197  9.076541e-01  5.154687e+01  0.946105        1           0
172.217.166.197  32    5234   204.238095  8.773237e+04  204.800000    5510.309937  0.172197  3.427576e-01  7.416773e+00  1.186071        1           0
142.250.194.170  16    1978   142.285714  4.051633e+03   53.666667    2755.154974  0.172197  5.033152e+00  1.459884e+02  0.826295        1           0
34.107.243.93     4     320    80.000000  1.960000e+02   28.000000     688.788749  0.172197  3.637180e-01  3.307270e-02  0.464584        1           0
34.107.221.82    36    3798   134.714286  1.162835e+04   79.692308    6199.098755  0.172197  2.399041e+00  1.343818e+02  0.782326        1           0
104.18.31.2       4     288    72.000000  3.600000e+01   12.000000     688.788730  0.172197  4.271642e-02  2.790865e-03  0.418125        1           0
140.82.112.26     8     636    80.000000  1.960000e+02   28.000000    1377.577506  0.172197  2.384186e-07  2.842171e-14  0.464584        1           0
216.58.200.174   67   13316   222.732143  8.656423e+04  212.654545   11537.211401  0.172197  2.045120e-01  1.960077e+01  1.293471        1           0
163.70.145.60    76   18786   311.666667  1.596074e+05  277.396226   13086.986112  0.172197  1.525566e-01  2.003907e+00  1.809941        1           0
142.250.194.182 458  599435  1322.355408  8.208590e+04   93.566372   78866.310447  0.172197  1.363645e-02  6.350573e+00  7.679309        1           0
142.250.182.174 549  352537   817.352697  9.470904e+05  252.458333   94536.255787  0.172197  7.252658e-02  1.625735e+01  4.746609        1           0
142.250.182.163  18   16007   642.333333  3.216182e+05  285.200000    3099.549388  0.172197  2.291961e-02  1.337828e-03  3.730220        1           0
142.250.195.1    71   46205   812.193548  3.306701e+05  431.833333   12226.000312  0.172197  1.693616e-01  2.927686e+00  4.716648        1           0
49.44.208.81   2144 2980347  1390.087220  1.057737e+04    6.861409  369190.763542  0.172197  2.392175e-03  3.957804e+00  8.072648        1           0
142.250.195.22   53   40655   788.913043  3.597189e+05  475.500000    9126.450939  0.172197  1.120394e-02  4.121456e-03  4.581451        1           0
142.250.77.234   43   21312   538.076923  3.425010e+05  298.789474    7404.478953  0.172197  1.991017e-02  3.643847e-02  3.124772        1           0
142.250.207.194  26    9073   412.619048  2.662477e+05  196.750000    4477.126828  0.172197  2.139732e-02  2.322605e-02  2.396201        1           0
49.44.208.76    403  547597  1358.801489  4.389654e+04   28.942786   69395.465432  0.172197  1.548808e-02  2.758755e-01  7.890962        1           0
142.250.206.106  84   14064   167.428571  5.570608e+04  154.373494   14464.563815  0.172197  5.716968e-01  1.489452e+02  0.972307        1           0
49.44.82.177     18   10244   569.111111  3.329184e+05  293.647059    3099.549420  0.172197  3.553395e-01  3.402039e+00  3.304997        1           0
49.44.184.206  1179 1629058  1381.728584  2.063578e+04   10.882003  203020.487404  0.172197  5.205695e-03  4.120318e-01  8.024106        1           0
49.44.184.205   211  855934  4056.559242  3.999289e+06  905.571429   36333.607204  0.172197  1.053991e-01  2.810167e+00 23.557639       -1           0
142.250.193.206  28    3862   137.928571  3.251085e+04  125.333333    4821.521386  0.172197  2.951365e-01  1.479848e+01  0.800992        1           0
No anomalies detected in the given time frame.
```

INCLUDING MODEL ACCURACY

```
please provide us feedback at https://github.com/pandas-dev/pandas/issues/54466

  import pandas as pd
Model Accuracy: 0.80
^CAlert! Potential DDoS attack detected from 192.168.31.179.
Blocked IP address: 192.168.31.179
Accumulating data...
                  TPC     TPL         APL            PLV         ALD            TPT       APT         ATD           PTV      Rate  Anomaly
192.168.31.179   1506  505781  335.843958  217505.507523  235.598007  259330.939014  0.172198    0.373174  19176.265340  1.950330        0
34.160.144.191      4     264   66.000000      72.000000   12.000000     688.793876  0.172198    0.007117      0.000088  0.383279        0
142.250.206.131   129   16095  124.767442   17010.783126   77.640625   22213.606954  0.172199    4.358153  21999.466154  0.724556        0
0.0.0.0            19    7066  371.894737       7.778393    3.666667    3271.771482  0.172198   29.832707  27271.690617  2.159686        0
192.168.31.144     90   21909  243.433333   20422.445556   80.561798   15497.864872  0.172198    6.015383  19501.693532  1.413679        0
104.18.31.2         2     132   66.000000       0.000000    0.000000     344.396943  0.172198    0.009220      0.000021  0.383279        0
34.107.221.82      50    4950   99.000000    6296.680000   29.877551    8609.924371  0.172198    6.179155  11422.615689  0.574918        0
192.168.31.1       64   11578  180.906250   11609.928711   65.603175   11020.704057  0.172199    8.492843  15348.608309  1.050568        0
142.250.195.3      79    9886  125.139241   16186.854030   78.692308   13603.679917  0.172198    2.302598   3704.170515  0.726715        0
142.250.193.78    158   33378  211.253165   78320.682743  129.872611   27207.361559  0.172198    3.008698  18985.187339  1.226800        0
142.250.206.170    47    8598  182.936170   86527.591670  175.608696    8093.328492  0.172198    3.040540   2406.526129  1.062356        0
142.251.12.84      37    6468  174.810811   70676.261505  164.111111    6371.343724  0.172198    3.598063   1618.167012  1.015170        0
185.125.190.17      4     461  115.250000    6520.687500  128.666667     688.793926  0.172198    0.269133      0.091998  0.669286        0
34.107.243.93       4     312   78.000000     144.000000   24.000000     688.793987  0.172198  100.093458  22525.030259  0.452966        0
172.217.166.197    31    6890  222.258065   91457.094693  211.800000    5338.153021  0.172198    2.335441    684.379866  1.290709        0
142.250.77.206     12    1751  145.916667   43436.576389  155.272727    2066.381841  0.172198    5.455285    861.046063  0.847375        0
13.107.5.93        24    6370  265.416667  126081.243056  269.304348    4132.763635  0.172198    0.267240      4.138348  1.541341        0
142.250.193.14    464   80516  173.525862   46309.538124  109.313175   79900.107493  0.172199    0.745523  11236.366414  1.007708        0
142.250.193.74    274   35216  128.525547   20799.577814   79.593407   47182.390362  0.172199    1.263820   8322.651746  0.746380        0
140.82.113.25      57   21272  373.192982  225378.331179  213.392857    9815.314252  0.172198    5.423565   6780.134069  2.167226        0
163.70.145.60     110   19778  179.800000   61271.741818  119.513761   18941.835024  0.172199    2.673666   7510.459466  1.044144        0
142.250.194.202    69   44649  647.086957  347439.238815  249.558824   11881.696547  0.172199    2.520855   1074.767467  3.757797        0
172.217.161.10     42   16448  391.619048  250392.378685  226.390244    7232.337345  0.172199    4.220893   2046.828419  2.274230        0
142.250.192.194    28   15497  553.464286  306551.105867  293.111111    4821.558253  0.172199    6.442118   1609.036461  3.214106        0
34.149.97.1        24   16071  669.625000  368581.317708  447.652174    4132.764282  0.172199    5.384318    854.266438  3.888681        0
34.117.188.166     21    9795  466.428571  296061.197279  445.500000    3616.168751  0.172199    6.191329    942.835130  2.708668        0
91.189.91.49        5     527  105.400000    5604.640000   92.500000     860.992557  0.172199    0.134907      0.039470  0.612084        0
192.168.31.189      4     808  202.000000   16584.500000  169.000000     688.794100  0.172199    0.073313      0.011372  1.173065        0
No anomalies detected in the given time frame.
himanshi@himanshi-HP-Pavilion-Gaming-Laptop-15-ec2xxx:~/Documents/sh$
```

ON IMPROVING MODEL ACCURACY

BEFORE ATTACK

```
  import pandas as pd
Model Accuracy: 1.00
Model Precision: 1.00
Model Recall: 1.00
Model F1-Score: 1.00
^CAccumulating data...
                TPC   TPL         APL          PLV        ALD         TPT       APT          ATD          PTV      Rate  Anomaly
192.168.31.79     9   756   84.000000     0.000000   0.000000  1549.808813  0.172201  3.587820e+00  8.729319e+01  0.487802        0
0.0.0.0           3  1116  372.000000     8.000000   3.000000   516.602936  0.172201  1.007383e+00  8.954959e-01  2.160266        1
192.168.31.1      2   727  363.500000   462.250000  43.000000   344.401957  0.172201  9.600091e-02  2.304044e-03  2.110906        0
192.168.31.179   36  3744  104.000000 10066.333333  80.828571  6199.235248  0.172201  3.570157e-01  3.959832e+00  0.603945        0
157.240.239.60    7   522   74.571429   111.673469  20.000000  1205.406853  0.172201  1.986821e-07  1.542893e-13  0.433049        0
34.149.97.1       3   237   79.000000   338.000000  19.500000   516.602937  0.172201  1.378059e-04  1.688045e-08  0.458766        0
34.107.221.82    15  1890  126.000000  8864.000000  96.000000  2583.014688  0.172201  7.832412e-01  6.881006e+00  0.731703        0
Potential anomaly detected from IP: 0.0.0.0
^CAccumulating data...
                TPC   TPL         APL          PLV        ALD         TPT       APT          ATD          PTV      Rate  Anomaly
192.168.31.79    20  3336   84.000000     0.000000   0.000000  3444.019603  0.172201  3.587820e+00  8.729319e+01  0.487802        0
0.0.0.0           3  1116  372.000000     8.000000   3.000000   516.602936  0.172201  1.007383e+00  8.954959e-01  2.160266        1
192.168.31.1      2   727  363.500000   462.250000  43.000000   344.401957  0.172201  9.600091e-02  2.304044e-03  2.110906        0
192.168.31.179   37  3810  104.000000 10066.333333  80.828571  6371.436229  0.172201  3.570157e-01  3.959832e+00  0.603945        0
157.240.239.60    7   522   74.571429   111.673469  20.000000  1205.406853  0.172201  1.986821e-07  1.542893e-13  0.433049        0
34.149.97.1       3   237   79.000000   338.000000  19.500000   516.602937  0.172201  1.378059e-04  1.688045e-08  0.458766        0
34.107.221.82    16  1956  126.000000  8864.000000  96.000000  2755.215669  0.172201  7.832412e-01  6.881006e+00  0.731703        0
Potential anomaly detected from IP: 0.0.0.0
^CAccumulating data...
                TPC   TPL         APL          PLV        ALD          TPT       APT          ATD          PTV      Rate  Anomaly
192.168.31.79    31  4260   84.000000     0.000000   0.000000  5338.230418  0.172201  3.587820e+00  8.729319e+01  0.487802        0
0.0.0.0           4  1486  372.000000     8.000000   3.000000   688.803921  0.172201  1.007383e+00  8.954959e-01  2.160266        1
192.168.31.1      2   727  363.500000   462.250000  43.000000   344.401957  0.172201  9.600091e-02  2.304044e-03  2.110906        0
192.168.31.179   62  7948  104.000000 10066.333333  80.828571 10676.460786  0.172201  3.570157e-01  3.959832e+00  0.603945        0
157.240.239.60   24  2804   74.571429   111.673469  20.000000  4132.823546  0.172201  1.986821e-07  1.542893e-13  0.433049        0
34.149.97.1       3   237   79.000000   338.000000  19.500000   516.602937  0.172201  1.378059e-04  1.688045e-08  0.458766        0
34.107.221.82    17  2022  126.000000  8864.000000  96.000000  2927.416652  0.172201  7.832412e-01  6.881006e+00  0.731703        0
Potential anomaly detected from IP: 0.0.0.0
The IP address 0.0.0.0 was detected as an anomaly 3 times.
himanshi@himanshi-HP-Pavilion-Gaming-Laptop-15-ec2xxx:~/Documents/sh$
History restored
```

ON IMPROVING MODEL ACCURACY AFTER ATTACK

```
                  TPC     TPL      APL          PLV         ALD          TPT       APT          ATD          PTV      Rate  Anomaly
192.168.43.91    9001  486054   54.000     0.000000    0.000000  1.550022e+06  0.172206  3.970816e-04  2.827843e-01  0.313579        1
192.168.43.87    9001  486054   54.000     0.000000    0.000000  1.550022e+06  0.172206  2.930561e-04  2.019490e-01  0.313579        1
142.250.194.99      1     105  105.000     0.000000    0.000000  1.722055e+02  0.172206  0.000000e+00  0.000000e+00  0.609737        0
157.240.198.60      3     340  137.000     0.000000    0.000000  5.166166e+02  0.172206  0.000000e+00  0.000000e+00  0.795561        0
216.58.221.42       2     132   66.000     0.000000    0.000000  3.444111e+02  0.172206  2.384186e-07  2.842171e-14  0.383263        0
142.250.206.110     2     132   66.000     0.000000    0.000000  3.444111e+02  0.172206  9.244967e-02  2.136735e-03  0.383263        0
142.250.77.238      8    1253  156.625 31132.484375  166.142857  1.377644e+03  0.172206  3.947259e-01  7.843034e-01  0.909524        0
192.168.43.1        1     195  195.000     0.000000    0.000000  1.722055e+02  0.172206  0.000000e+00  0.000000e+00  1.132368        0
Potential anomaly detected from IP: 192.168.43.91
Potential anomaly detected from IP: 192.168.43.87
^CAccumulating data...
                  TPC     TPL      APL          PLV         ALD          TPT       APT          ATD          PTV      Rate  Anomaly
192.168.43.91    9001  486054   54.000     0.000000    0.000000  1.550022e+06  0.172206  3.970816e-04  2.827843e-01  0.313579        1
192.168.43.87    9001  486054   54.000     0.000000    0.000000  1.550022e+06  0.172206  2.930561e-04  2.019490e-01  0.313579        1
142.250.194.99      3     237  105.000     0.000000    0.000000  5.166166e+02  0.172206  0.000000e+00  0.000000e+00  0.609737        0
157.240.198.60     10    1241  137.000     0.000000    0.000000  1.722055e+03  0.172206  0.000000e+00  0.000000e+00  0.795561        0
216.58.221.42       2     132   66.000     0.000000    0.000000  3.444111e+02  0.172206  2.384186e-07  2.842171e-14  0.383263        0
142.250.206.110     2     132   66.000     0.000000    0.000000  3.444111e+02  0.172206  9.244967e-02  2.136735e-03  0.383263        0
142.250.77.238      8    1253  156.625 31132.484375  166.142857  1.377644e+03  0.172206  3.947259e-01  7.843034e-01  0.909524        0
192.168.43.1        3     873  195.000     0.000000    0.000000  5.166166e+02  0.172206  0.000000e+00  0.000000e+00  1.132368        0
91.189.91.49        4     461  115.250  6520.687500  123.333333  6.888221e+02  0.172206  4.437956e-01  2.222264e-01  0.669258        0
185.125.190.57      1      90   90.000     0.000000    0.000000  1.722055e+02  0.172206  0.000000e+00  0.000000e+00  0.522631        0
142.250.194.130     1     105  105.000     0.000000    0.000000  1.722055e+02  0.172206  0.000000e+00  0.000000e+00  0.609736        0
Potential anomaly detected from IP: 192.168.43.91
Potential anomaly detected from IP: 192.168.43.87
The IP address 192.168.43.91 was detected as an anomaly 2 times.
```

MITIGATION

BLOCKING OF IP

CODE OF BLOCK FUNCTION

```
packet_counts = defaultdict(int)
packet_times = defaultdict(list)
ip_occurrences = Counter()
anomaly_ips = []

def block_ip(ip_address):
    try:
        subprocess.run(['sudo', 'iptables', '-A', 'INPUT', '-s', ip_address, '-j', 'DROP'], check=True)
        print(f"Blocked IP address: {ip_address}")
    except subprocess.CalledProcessError as e:
        print(f"Failed to block IP address {ip_address}: {e}")

# Load training data from CSV
def load_training_data(csv_file):
    df = pd.read_csv(csv_file)
    df.reset_index(drop=True, inplace=True)  # Reset index to default integer index
    X = df[['TPC', 'TPL', 'APL', 'PLV', 'ALD', 'TPT', 'APT', 'ATD', 'PTV', 'Rate']]
    y = [0] * len(X)  # Label all training data as normal (0)
```

BLOCKING OF IP

WILL ASK TO BLOCK INCASE OF ANOMALY

```
    # Identify and collect potential anomalies
    for ip, anomaly in zip(df.index, df['Anomaly']):
        if anomaly == 1:  # Random Forest marks anomalies with 1
            print(f"Potential anomaly detected from IP: {ip}")
            anomaly_ips.append(ip)

# Determine the most frequent anomaly IP
if anomaly_ips:
    most_common_anomaly_ip, anomaly_count = Counter(anomaly_ips).most_common(1)[0]
    print(f"IP address with the most frequent anomalies: {most_common_anomaly_ip} (Count: {anomaly_count})")
    user_input = input(f"Do you want to block IP address {most_common_anomaly_ip}? (yes/no): ")
    if user_input.lower() == 'yes':
        block_ip(most_common_anomaly_ip)
else:
    print("No anomalies detected in the given time frame.")

__name__ == "__main__":
main()
```

BLOCKING OF IP

OUTPUT WHEN THERE IS ATTACK

```
  import pandas as pd
Model Accuracy: 0.80
Alert! Potential DDoS attack detected from 104.18.30.2.
Blocked IP address: 104.18.30.2
Alert! Potential DDoS attack detected from 192.168.31.179.
Blocked IP address: 192.168.31.179
Alert! Potential DDoS attack detected from 104.18.30.2.
Blocked IP address: 104.18.30.2
Alert! Potential DDoS attack detected from 192.168.31.179.
Blocked IP address: 192.168.31.179
Alert! Potential DDoS attack detected from 104.18.30.2.
Blocked IP address: 104.18.30.2
Alert! Potential DDoS attack detected from 104.18.30.2.
Blocked IP address: 104.18.30.2
Alert! Potential DDoS attack detected from 192.168.31.179.
Blocked IP address: 192.168.31.179
Alert! Potential DDoS attack detected from 104.18.30.2.
Blocked IP address: 104.18.30.2
Alert! Potential DDoS attack detected from 192.168.31.179.
Blocked IP address: 192.168.31.179
Accumulating data...
                  TPC      TPL          APL           PLV         ALD           TPT       APT       ATD          PTV      Rate  Anomaly
104.18.30.2      5312  7671908  1444.259789  710202.379046  639.748635  914717.967388  0.172198  0.018449   387.134296  8.387184        0
192.168.31.179   4113   422674   102.765378   38348.739263   27.429475  708252.071673  0.172198  0.023828   430.867278  0.596785        0
142.250.206.131    37     3845   103.918919    1157.371804   31.833333    6371.341255  0.172198  2.673292  1294.299580  0.603484        0
34.120.208.123      3      237    79.000000     338.000000   19.500000     516.595237  0.172198 26.891049   642.769929  0.458773        0
192.168.31.144    127    23440   184.566929   20926.670717   31.857143   21869.198483  0.172198  0.759051   809.403641  1.071827        0
192.168.31.189     14     4102   293.000000   24318.000000  100.923077    2410.777752  0.172198  4.404498   130.962946  1.701526        0
142.250.193.46    126    18847   149.579365   26838.211955  100.784000   21697.000158  0.172198  0.726245   874.110398  0.868645        0
192.168.31.12       5      760   152.000000       0.000000    0.000000     860.992054  0.172198  0.511833     0.710496  0.882703        0
216.58.200.174     45     8284   184.088889   32407.947654  124.113636    7748.928727  0.172198  0.753236    22.901942  1.069051        0
192.168.31.1       12     1581   131.750000    2053.854167   20.363636    2066.380995  0.172198  3.692423   153.308689  0.765106        0
40.74.98.193       11     5932   539.272727  279176.016529  342.000000    1894.182557  0.172198  0.070657     0.041707  3.131694        0
142.250.192.202    28     5823   207.964286  100274.820153  252.518519    4821.555651  0.172198  0.053087     0.259497  1.207702        0
142.251.175.84     16     4203   262.687500  118053.339844  282.666667    2755.174673  0.172198  0.040951     0.020308  1.525493        0
No anomalies detected in the given time frame.
himanshi@himanshi-HP-Pavilion-Gaming-Laptop-15-ec2xxx:~/Documents/sh$
```

BLOCKING OF IP

OUTPUT WHEN THERE IS ANOMALY

```
  import pandas as pd
Model Accuracy: 1.00
^CAccumulating data...
                  TPC    TPL         APL            PLV         ALD           TPT       APT        ATD         PTV      Rate  Anomaly
192.168.31.144      1    179  179.000000       0.000000    0.000000    172.199136  0.172199   0.000000    0.000000  1.039494        1
192.168.31.179    124  26601  214.524194  120987.281673  121.024390  21352.693328  0.172199   0.468716  490.269888  1.245791        0
49.44.196.102       6    408   68.000000      20.000000    2.400000   1033.194824  0.172199   2.544293   23.094582  0.394892        0
34.107.221.82      10   1406  140.600000   12659.240000   44.000000   1721.991406  0.172199   6.169883  602.527951  0.816497        0
185.125.190.98      4    457  114.250000    6244.187500  126.000000    688.796550  0.172199   0.135299    0.020596  0.663476        0
192.168.31.1       14   2475  176.785714    3173.025510   37.307692   2410.787969  0.172199   3.683444  327.173924  1.026635        0
20.189.173.1       24  12008  500.333333  277630.555556  490.782609   4132.779301  0.172199   0.084896    0.191068  2.905551        0
34.107.243.93       4    342   85.500000     380.250000   13.000000    688.796564  0.172199  15.176829  388.692227  0.496518        0
34.117.188.166      6    498   83.000000     266.000000   10.200000   1033.194849  0.172199   8.348040  240.554431  0.482000        0
185.125.190.56      1     90   90.000000       0.000000    0.000000    172.199140  0.172199   0.000000    0.000000  0.522651        0
142.250.192.206     4    342   85.500000     380.250000   39.000000    688.796567  0.172199   4.975228   41.769516  0.496518        0
142.250.192.174     3    276   92.000000     338.000000   19.500000    516.597425  0.172199   5.519973   27.084536  0.534265        0
52.182.143.209     10   5866  586.600000  288499.640000  361.777778   1721.991414  0.172199   0.204481    0.302647  3.406521        0
Potential anomaly detected from IP: 192.168.31.144
IP address with the most frequent anomalies: 192.168.31.144 (Count: 1)
Do you want to block IP address 192.168.31.144? (yes/no): no
```

FINAL OUTPUT ON PERFORMING DDOS ATTACK

```
Model Accuracy: 1.00
Model Precision: 1.00
Model Recall: 1.00
Model F1-Score: 1.00
Accumulating data...
            TPC    TPL  APL  PLV  ALD         TPT     APT     ATD     PTV    Rate  Anomaly
192.168.43.91  4267  230418  54.0  0.0  0.0  734800.985361  0.172206  0.000397  0.282784  0.313579       0
192.168.43.87  5731  309474  54.0  0.0  0.0  986909.877508  0.172206  0.000293  0.201949  0.313579       0
Alert! Potential DDoS attack detected from 192.168.43.87.
Blocked IP address: 192.168.43.87
Alert! Potential DDoS attack detected from 192.168.43.91.
Blocked IP address: 192.168.43.91
Accumulating data...
            TPC    TPL   APL  PLV  ALD         TPT     APT     ATD     PTV    Rate  Anomaly
192.168.43.91   9001  486054   54.0  0.0  0.0  1.550022e+06  0.172206  0.000397  0.282784  0.313579       0
192.168.43.87   9001  486054   54.0  0.0  0.0  1.550022e+06  0.172206  0.000293  0.201949  0.313579       0
142.250.194.99     1     105  105.0  0.0  0.0  1.722055e+02  0.172206  0.000000  0.000000  0.609737       0
Accumulating data...
            TPC    TPL   APL  PLV  ALD         TPT     APT     ATD     PTV    Rate  Anomaly
192.168.43.91   9001  486054   54.0  0.0  0.0  1.550022e+06  0.172206  0.000397  0.282784  0.313579       0
192.168.43.87   9001  486054   54.0  0.0  0.0  1.550022e+06  0.172206  0.000293  0.201949  0.313579       0
142.250.194.99     1     105  105.0  0.0  0.0  1.722055e+02  0.172206  0.000000  0.000000  0.609737       0
Accumulating data...
            TPC    TPL   APL  PLV  ALD         TPT     APT     ATD     PTV    Rate  Anomaly
192.168.43.91   9001  486054   54.0  0.0  0.0  1.550022e+06  0.172206  0.000397  0.282784  0.313579       0
192.168.43.87   9001  486054   54.0  0.0  0.0  1.550022e+06  0.172206  0.000293  0.201949  0.313579       0
142.250.194.99     1     105  105.0  0.0  0.0  1.722055e+02  0.172206  0.000000  0.000000  0.609737       0
Accumulating data...
            TPC    TPL   APL  PLV  ALD         TPT     APT     ATD     PTV    Rate  Anomaly
192.168.43.91   9001  486054   54.0  0.0  0.0  1.550022e+06  0.172206  0.000397  0.282784  0.313579       0
192.168.43.87   9001  486054   54.0  0.0  0.0  1.550022e+06  0.172206  0.000293  0.201949  0.313579       0
142.250.194.99     1     105  105.0  0.0  0.0  1.722055e+02  0.172206  0.000000  0.000000  0.609737       0
Accumulating data...
            TPC    TPL   APL  PLV  ALD         TPT     APT     ATD     PTV    Rate  Anomaly
192.168.43.91   9001  486054   54.0  0.0  0.0  1.550022e+06  0.172206  0.000397  0.282784  0.313579       0
192.168.43.87   9001  486054   54.0  0.0  0.0  1.550022e+06  0.172206  0.000293  0.201949  0.313579       0
142.250.194.99     1     105  105.0  0.0  0.0  1.722055e+02  0.172206  0.000000  0.000000  0.609737       0
Accumulating data...
            TPC    TPL   APL  PLV  ALD         TPT     APT     ATD     PTV    Rate  Anomaly
192.168.43.91   9001  486054   54.0  0.0  0.0  1.550022e+06  0.172206  0.000397  0.282784  0.313579       0
192.168.43.87   9001  486054   54.0  0.0  0.0  1.550022e+06  0.172206  0.000293  0.201949  0.313579       0
142.250.194.99     1     105  105.0  0.0  0.0  1.722055e+02  0.172206  0.000000  0.000000  0.609737       0
157.240.198.60     1     137  137.0  0.0  0.0  1.722055e+02  0.172206  0.000000  0.000000  0.795561       0
Accumulating data...
            TPC    TPL   APL  PLV  ALD         TPT     APT     ATD     PTV    Rate  Anomaly
192.168.43.91   9001  486054   54.0  0.0  0.0  1.550022e+06  0.172206  0.000397  0.282784  0.313579       0
192.168.43.87   9001  486054   54.0  0.0  0.0  1.550022e+06  0.172206  0.000293  0.201949  0.313579       0
142.250.194.99     1     105  105.0  0.0  0.0  1.722055e+02  0.172206  0.000000  0.000000  0.609737       0
157.240.198.60     1     137  137.0  0.0  0.0  1.722055e+02  0.172206  0.000000  0.000000  0.795561       0
Accumulating data...
            TPC    TPL   APL  PLV  ALD         TPT     APT     ATD     PTV    Rate  Anomaly
192.168.43.91   9001  486054   54.0  0.0  0.0  1.550022e+06  0.172206  0.000397  0.282784  0.313579       0
192.168.43.87   9001  486054   54.0  0.0  0.0  1.550022e+06  0.172206  0.000293  0.201949  0.313579       0
142.250.194.99     1     105  105.0  0.0  0.0  1.722055e+02  0.172206  0.000000  0.000000  0.609737       0
157.240.198.60     1     137  137.0  0.0  0.0  1.722055e+02  0.172206  0.000000  0.000000  0.795561       0
Accumulating data...
            TPC    TPL   APL  PLV  ALD         TPT     APT     ATD     PTV    Rate  Anomaly
192.168.43.91   9001  486054   54.0  0.0  0.0  1.550022e+06  0.172206  0.000397  0.282784  0.313579       0
192.168.43.87   9001  486054   54.0  0.0  0.0  1.550022e+06  0.172206  0.000293  0.201949  0.313579       0
142.250.194.99     1     105  105.0  0.0  0.0  1.722055e+02  0.172206  0.000000  0.000000  0.609737       0
157.240.198.60     1     137  137.0  0.0  0.0  1.722055e+02  0.172206  0.000000  0.000000  0.795561       0
Accumulating data...
            TPC    TPL   APL  PLV  ALD         TPT     APT     ATD     PTV    Rate  Anomaly
192.168.43.91   9001  486054   54.0  0.0  0.0  1.550022e+06  0.172206  0.000397  0.282784  0.313579       0
192.168.43.87   9001  486054   54.0  0.0  0.0  1.550022e+06  0.172206  0.000293  0.201949  0.313579       0
142.250.194.99     1     105  105.0  0.0  0.0  1.722055e+02  0.172206  0.000000  0.000000  0.609737       0
157.240.198.60     1     137  137.0  0.0  0.0  1.722055e+02  0.172206  0.000000  0.000000  0.795561       0
Accumulating data...
            TPC    TPL   APL  PLV  ALD         TPT     APT     ATD     PTV    Rate  Anomaly
192.168.43.91   9001  486054   54.0  0.0  0.0  1.550022e+06  0.172206  0.000397  0.282784  0.313579       0
192.168.43.87   9001  486054   54.0  0.0  0.0  1.550022e+06  0.172206  0.000293  0.201949  0.313579       0
142.250.194.99     1     105  105.0  0.0  0.0  1.722055e+02  0.172206  0.000000  0.000000  0.609737       0
157.240.198.60     1     137  137.0  0.0  0.0  1.722055e+02  0.172206  0.000000  0.000000  0.795561       0
^CAccumulating data...
            TPC    TPL    APL        PLV      ALD        TPT     APT        ATD        PTV    Rate  Anomaly
192.168.43.91   9001  486054   54.000     0.000000   0.000000  1.550022e+06  0.172206  3.970816e-04  2.827843e-01  0.313579       1
192.168.43.87   9001  486054   54.000     0.000000   0.000000  1.550022e+06  0.172206  2.930561e-04  2.019490e-01  0.313579       1
142.250.194.99     1     105  105.000     0.000000   0.000000  1.722055e+02  0.172206  0.000000e+00  0.000000e+00  0.609737       0
157.240.198.60     3     340  137.000     0.000000   0.000000  5.166166e+02  0.172206  0.000000e+00  0.000000e+00  0.795561       0
216.58.221.42      2     132   66.000     0.000000   0.000000  3.444111e+02  0.172206  2.384186e-07  2.842171e-14  0.383263       0
142.250.206.110    2     132   66.000     0.000000   0.000000  3.444111e+02  0.172206  9.244967e-02  2.136735e-03  0.383263       0
142.250.77.238     8    1253  156.625  31132.484375  166.142857  1.377644e+03  0.172206  3.947259e-01  7.843034e-01  0.909524       0
192.168.43.1       1     195  195.000     0.000000   0.000000  1.722055e+02  0.172206  0.000000e+00  0.000000e+00  1.132368       0
Potential anomaly detected from IP: 192.168.43.91
Potential anomaly detected from IP: 192.168.43.87
^CAccumulating data...
            TPC    TPL    APL        PLV      ALD        TPT     APT        ATD        PTV    Rate  Anomaly
192.168.43.91   9001  486054   54.000     0.000000   0.000000  1.550022e+06  0.172206  3.970816e-04  2.827843e-01  0.313579       1
192.168.43.87   9001  486054   54.000     0.000000   0.000000  1.550022e+06  0.172206  2.930561e-04  2.019490e-01  0.313579       1
142.250.194.99     3     237  105.000     0.000000   0.000000  5.166166e+02  0.172206  0.000000e+00  0.000000e+00  0.609737       0
157.240.198.60    10    1241  137.000     0.000000   0.000000  1.722055e+03  0.172206  0.000000e+00  0.000000e+00  0.795561       0
216.58.221.42      2     132   66.000     0.000000   0.000000  3.444111e+02  0.172206  2.384186e-07  2.842171e-14  0.383263       0
142.250.206.110    2     132   66.000     0.000000   0.000000  3.444111e+02  0.172206  9.244967e-02  2.136735e-03  0.383263       0
142.250.77.238     8    1253  156.625  31132.484375  166.142857  1.377644e+03  0.172206  3.947259e-01  7.843034e-01  0.909524       0
192.168.43.1       3     873  195.000     0.000000   0.000000  5.166166e+02  0.172206  0.000000e+00  0.000000e+00  1.132368       0
91.189.91.49       4     461  115.250   6520.687500  123.333333  6.888221e+02  0.172206  4.437956e-01  2.222264e-01  0.669258       0
185.125.190.57     1      90   90.000     0.000000   0.000000  1.722055e+02  0.172206  0.000000e+00  0.000000e+00  0.522631       0
142.250.194.130    1     105  105.000     0.000000   0.000000  1.722055e+02  0.172206  0.000000e+00  0.000000e+00  0.609736       0
Potential anomaly detected from IP: 192.168.43.91
Potential anomaly detected from IP: 192.168.43.87
The IP address 192.168.43.91 was detected as an anomaly 2 times.
```

WEBSITES USED

- Kasperky: What is a Packet Sniffer? (kaspersky.com)
- Gadget Review_: How to Scan Router for Viruses | Scanning Router For Malware (gadgetreview.com)
- Springer Link: Classification of packet contents for malware detection | Journal of Computer Virology and Hacking Techniques (springer.com)

THANK YOU