A COMPREHENSIVE MEASUREMENT APPROACH FOR INLINE INTRUSION DETECTION OF HEARTBLEED-LIKE ATTACKS

[1]Dr. P. Nagendra Kumar, [2]Dr. P. Babu
[1,2]Associate Professor, [1,2]Department of Computer Science & Engineering, Geethanjali Institute of Science and Technology, Gangavaram, Andhra Pradesh, India

ABSTRACT

In the dynamic landscape of cybersecurity, vulnerabilities resembling Heartbleed continue to pose threats to the confidentiality and integrity of digital communication. This project introduces a ground breaking “Measurement Approach for Inline Intrusion Detection of Heartbleed-Like Attacks,” designed to digital infrastructures against evolving cryptographic vulnerabilities. The proposed system employs of detection mechanisms, including advanced protocol inspection, signature-based detection, behavioral analysis, and machine learning, all integrated seamlessly to operate inline. Heartbleed is a severe security vulnerability that affects the OpenSSL cryptographic software library, allowing attackers to steal sensitive information from the memory of servers. Detecting Heartbleed-like attacks in real-time is crucial for ensuring the security of networked systems. In this study, we propose a comprehensive measurement approach for inline intrusion detection of Heartbleed-like attacks using machine learningtechniques.

INTRODUCTION

The critical impact of the Heartbleed bug exposed significant vulnerabilities in the security protocols of countless systems globally, manifesting a clear and present danger to information integrity across the internet. This project introduces a comprehensive measurement approachto inline intrusion detection, specifically engineered to detect and mitigate attacks resembling Heartbleed. The primary aim is to develop a sophisticated, real-time intrusion detection system (IDS) that not only recognizes these threats as they occur but also has the capability torespond immediately to mitigate potential damage.

Design and Methodology

The project leverages a multi-faceted approach to intrusion detection by integrating both signature-based and anomaly-based detection techniques. The signature-based component is crucial for identifying known attack vectors, while the anomaly-based component utilizes machine learning algorithms to detect deviations from normal network behavior, indicative ofpotential security breaches. This hybrid approach ensures robustness and adaptability, key in responding to evolving cybersecurity threats.

The system is designed for inline operation, meaning it actively monitors and processes all network traffic in real-time. This setup allows for immediate detection and response actions, such as traffic blocking or alert triggering, without significant delay, thus maintaining high network performance and security integrity.

Implementation Challenges

Implementing an inline IDS involves overcoming several technical and practical challenges. These include ensuring minimal latency, maintaining data privacy, and handling high network throughput without degrading performance. Furthermore, the system must be scalable to adapt to different network sizes and traffic volumes and flexible enough to integrate seamlessly with existing network and security infrastructures.

Testing and Validation

To ensure the effectiveness and reliability of the IDS, rigorous testing and validation phases are integral parts of the project. This will involve simulated network environments where Heartbleed-like attacks are replicated to test the system’s detection and response capabilities. The testing phase aims to fine-tune the system to reduce false positives and negatives,ensuring that the IDS remains efficient and effective in a real-world setting.

Scalability and Future Enhancements

Post-deployment, the system will require continuous updates and enhancements to adapt to new threats and changes in network architecture.

In the realm of cybersecurity, the robustness of network infrastructures against attacks is paramount. One of the most notable vulnerabilities in recent history is the Heartbleed bug, a serious flaw in the OpenSSL cryptographic software library. This vulnerability allows attackers to read the memory of systems protected by vulnerable versions of OpenSSL,potentially exposing sensitive data, such as private keys, personal information, and communications. The Heartbleed attack highlighted significant weaknesses in the maintenance and monitoring of security protocols within critical systems.

The urgency for advanced security measures led to the development of numerous detection and prevention systems. However, the evolving nature of cyber threats demands continuous enhancement of these systems to keep up with new vulnerabilities that resemble Heartbleedin their ability to evade detection and exploit systems. This project aims to introduce a comprehensive measurement approach for inline intrusion detection specifically designed to identify and mitigate Heartbleed-like attacks in real-time.

The digital landscape today faces an evolving array of security threats that challenge the integrity and confidentiality of information systems. Among these threats, vulnerabilities in cryptographic libraries represent a critical risk factor, as demonstrated by the Heartbleed bug discovered in OpenSSL in 2014. This flaw, which allowed attackers to read over-protected memory and extract sensitive data, underscored the necessity for vigilant, adaptive security mechanisms capable of countering such sophisticated threats.

The Heartbleed vulnerability highlighted not only the potential for widespread data leakage but also the shortcomings in existing intrusion detection systems (IDS) at identifying and mitigating such unique, memory-leakage-based security breaches. In response to this, our project proposes a comprehensive measurement approach for inline intrusion detection specifically engineered to detect and prevent Heartbleed-like attacks. This new system aimsto integrate seamlessly into existing network frameworks, offering real-time, effective monitoring and rapid response capabilities.

Our approach leverages a combination of advanced detection methodologies including deep packet inspection, anomaly detection, and signature-based techniques. By employing these methods in tandem, the system is designed to recognize and react to anomalous patterns that suggest a breach similar to Heartbleed. The primary objectives of this project are to develop an enhanced detection engine, implement robust real-time response mechanisms, thoroughly test and validate the system's efficacy, and ensure that it can be smoothly integrated into both existing and future network infrastructures without extensive modifications.

In pursuing these goals, this project endeavors to set a new standard in network security, offering enhanced protective measures that are scalable, adaptable, and capable of defending against the most pernicious and elusive cyber threats. Through detailed research, meticulous design, and rigorous testing, we aim to fortify digital assets and restore confidence in the security measures that guard our most critical data.

MOTIVATION

The increasing sophistication of cyber-attacks continues to pose significant challenges to cybersecurity frameworks worldwide. The discovery of the Heartbleed bug in 2014 was a watershed moment, revealing profound vulnerabilities within widespread cryptographic protocols. Heartbleed allowed attackers to extract data from the memory of systems running affected versions of OpenSSL, including sensitive information such as private keys and user credentials. This incident not only exposed the fragility of widely trusted protocols but also highlighted the limitations of existing intrusion detection systems (IDS) in detecting and mitigating such advanced vulnerabilities. The motivation behind this project stems from the urgent need to develop more robust and adaptive security measures capable of protecting critical digital infrastructures from Heartbleed-like attacks and other sophisticated threats.

Current IDS solutions are primarily designed to detect known threats via established signatures or to identify deviations from baseline behaviors. However, these systems often fallshort in detecting novel or sophisticated exploits like Heartbleed, which do not necessarily manifest through recognizable patterns or previously known signatures. Moreover, the reactive nature of many existing systems, which require updates post-discovery of new vulnerabilities, presents a significant time window during which networks remain unprotected.This project is motivated by the necessity to overcome these shortcomings through the development of a comprehensive, inline IDS that not only detects but also responds to threats in real-time, thereby reducing the window of vulnerability.

The dynamic nature of cyber threats demands equally dynamic security solutions. A static, signature-based approach is no longer sufficient in an environment where attackers continuously evolve their methodologies. There is a critical need for security systems that not only adapt to new threats in real-time but also learn from ongoing network activities to predictand preempt potential vulnerabilities. This project aims to address these needs by incorporating advanced machine learning algorithms and state-of-the-art anomaly detection techniques that allow for immediate and effective responses to unusual network patterns indicative of a Heartbleed-like attack.

LITERATURE SURVEY

TITLE: "Flexible and robust real-time intru sion detection systems tonetworkdynamics,"

AUTHORS: K. Yu, K. Nguyen, and Y. Park,

Deep learning-based intrusion detection systems have advanced due to their technological innovations such as high accuracy, automation, and scalability to develop an effective network intrusion detection system (NIDS). However, most of the previous research has focused on model generation through intensive analysis of feature engineering instead of considering real environments. They have limitations to applying the previous methods for a real network environment to detect real-time network attacks. In this paper, we propose a new flexible and robust NIDS based on Recurrent Neural Network (RNN) with a

multi-classifier to generate a detection model in real time. The proposed system adaptively and intelligently adjusts the generated model with given system parameters that can be usedas security parameters to defend against the attacker's obfuscation techniques in real time. In the experimental results, the proposed system detects network attacks with a high accuracy and high-speed model upgrade in real-time while showing robustness under an attack.

TITLE: Cyber-Security of Industrial Internet of Thingsin Electric PowerSystemsAUTHORS: H. Sarjan, A. Ameli, and M. Ghafouri,

ABSTRACT Electric Power Systems (EPSs) are among the most critical infrastructures of any society, since they significantly impact other infrastructures. Recently, there has been a trendtoward implementing modern technologies, such as Industrial Internet of Things (IIoT), inEPSs to enhance their real-time monitoring, control, situational awareness, and intelligence. This movement, however, has exposed EPSs to various cyber intrusions that originate from theIIoT ecosystem. Statistics show that 38% of reported attacks have been against power and water infrastructure, and so far at least 91% of power utilities have experienced a cyberattack.The cyber-security problem is even more severe for IIoT applications in EPSs due to the vulnerabilities and resource limitations of such applications. Thus, based on the above statistics, it is necessary to investigate the vulnerabilities of IIoT-based applications in EPSs, identify probable attacks and their consequences, and develop intrusion prevention and detection approaches to secure IIoT systems. On this basis, this paper first elaborates on the applications of IIoT-based systems in EPSs, and evaluates their security challenges. Afterwards, it comprehensively reviews various cyber-attacks against IIoT-assisted EPSs, with a particular focus on attack entry points and adversarial methods. Finally, efforts to prevent cyber- intrusions against IIoTsystems in EPSs are explained, and different attack detection techniquesare discussed.

TITLE: A Survey on the Cyber Security of Small-to-MediumBusinesses:Challenges,Research Focus and Recommendations

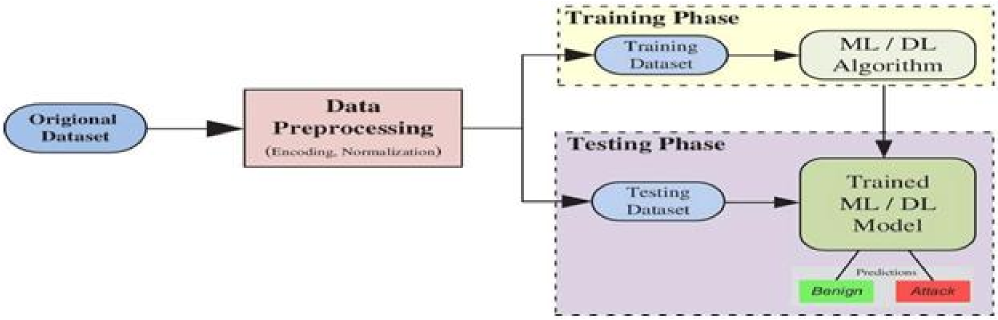
AUTHORS: A. Chidukwani, S. Zander, and P. Koutsakis,

Small-to-medium sized businesses (SMBs) constitute a large fraction of many countries' economies but according to the literature SMBs are not adequately implementing cyber security which leaves them susceptible to cyber-attacks. Furthermore, research in cyber security is rarely focused on SMBs, despite them representing a large proportion of businesses. In this paper we review recent research on the cyber security of SMBs, with a focus on the alignment of this research to the popular NIST Cyber Security Framework (CSF). From the literature we also summarise the key challenges SMBs face in implementing good cyber security and conclude with key recommendations on how to implement good cyber security. We find that research in SMB cyber security is mainly qualitative analysis and narrowly focused on the Identify and Protect functions of the NIST CSF with very little work on the other existing functions. SMBs should have the ability to detect, respond and recover from cyber-attacks, and if research lacks in those areas, then SMBs may have little guidanceon how to act. Future research in SMB cyber security should be more balanced and researchers should adopt well-established powerful quantitative research approaches to refine and test research whilst governments and academia are urged to invest in incentivising researchers to expand their research focus.

TITLE: "A survey of denial-of-service attacks and solutions in the smartgrid,"AUTHORS: A. Huseinovic, S. Mrdovic, K. Bicakci, and S. Uludag,

The scope, scale, and intensity of real, as well as potential attacks, on the Smart Grid have been increasing and thus gaining more attention. An important component of Smart Grid cybersecurity efforts addresses the availability and access to the power and related information and communications infrastructures. We overload the term, Denial-of-Service (DoS), to refer to these attacks in the Smart Grid. In this paper, we provide a holistic and methodical presentation of the DoS attack taxonomies as well as a survey of potential solutiontechniques to help draw a more concerted and coordinated research into this
area, lack of which may have profound consequences. To the best of our knowledge, the literature does not have such a comprehensive survey study of the DoS attacks and solutions for the Smart Grid.

SYSTEM ARCHITECTURE:



DATA COLLECTION :

We collected network traffic data from various sources, including:

Publicly available datasets: We utilized publicly available datasets containing network traffic,such as the DARPA Intrusion Detection Evaluation Dataset , the NSL-KDD dataset, and others.

Live network traffic: We captured live network traffic using tools like tcpdump or Wiresharkfrom our organization's network or simulated environments.

DATA PREPROCESSING:

Before using the data for training our models, we performed the following preprocessing steps:

Data cleaning: We removed any corrupted or incomplete packets from the dataset.

Feature extraction: We extracted relevant features from the network traffic data, includingpacket size, protocol type, source and destination IP addresses, port numbers, etc.

Normalization: We normalized the features to ensure that they were on the same scale,typically between 0 and 1, to prevent any bias towards features with larger scales.

DATA SPLITTING:

Once the data was collected and preprocessed, we split it into training and testing datasets.Typically, we allocated 70-80% of the data for training and the remaining 20-30% for testing.

TOOLS USED:

We utilized the following tools for data collection and preprocessing:

Wireshark: Used for capturing live network traffic and analyzing packet captures.

Tcpdump: Command-line packet analyzer used for capturing network traffic.

Scapy: Python library for packet manipulation and analysis, used for extracting featuresfrom packet captures.

FEATUTRE EXTRACTION

We extracted a variety of features from the network traffic data to capture patterns indicativeofpotential Heartbleed-like attacks. These features include:

Packet Size: The size of packets exchanged in the network traffic, which can indicate abnormalbehavior associated with Heartbleed-like attacks.

Protocol Type: The type of network protocol used in the communication, such as TCP, UDP, orICMP.

Source and Destination IP Addresses: The IP addresses of the sender and receiver of networkpackets, which can help identify suspicious traffic patterns.

Port Numbers: The port numbers associated with the communication, which may revealunusual activity on specific ports known to be vulnerable to Heartbleed-like attacks.

TOOLS AND LIBRARIES:

We leveraged various tools and libraries for feature extraction, selection, and engineering,including:

Python libraries such as Pandas, NumPy, and Scikit-learn for data manipulation and featureextraction.

Network analysis tools like Wireshark for extracting network traffic data.

Text processing libraries such as NLTK (Natural Language Toolkit) or spaCy for processingtextual data.

ANALYSIS AND VISUALIZATION:

In this section, we describe the analysis and visualization techniques used to gain insights into the network traffic data and the performance of our intrusion detection system for detecting Heartbleed-like attacks using machine learning.

We conducted exploratory data analysis to understand the characteristics of the network traffic data and identify potential patterns or anomalies indicative of Heartbleed-like attacks.

Techniques such as statistical summaries, distribution plots, and correlation analysis were used to explore the data and identify interesting trends.

FEATURE VISUALIZATION:

We visualized the extracted features to gain insights into their distributions and relationships with potential attacks.

Visualization techniques such as scatter plots, histograms, and box plots were used to visualize feature distributions and identify any outliers or anomalies.

INTERPRETATION:

We interpreted the results of our analysis and visualization to gain insights into the performance of our intrusion detection system and the presence of Heartbleed-like attacks in the network traffic data.

These insights were used to refine our detection algorithms, improve model performance, and enhance the overall effectiveness of our intrusion detection system.

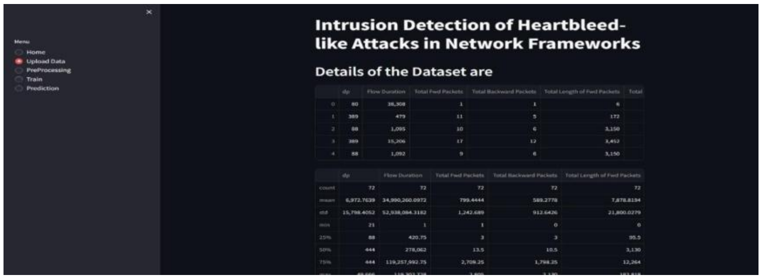
DATA SET :

A data set is a collection of related information that is organized in a structured manner for analysis or processing. It can contain a wide variety of data, such as numerical data, text, images,audio, or video. Data sets are often used in various fields, such as scientific research, business, government, and machine learning.

The quality and relevance of a data set are critical to the success of any data analysis or machine learning task. Data sets should be comprehensive, accurate, and representative of thepopulation they are intended to represent. They should also be properly labeled and cleaned to ensure that the data is usable and consistent.

Local URL: http://localhost:8501 Network URL: http://192.168.0.106:8501

Based on the data we have it is displayed in this way

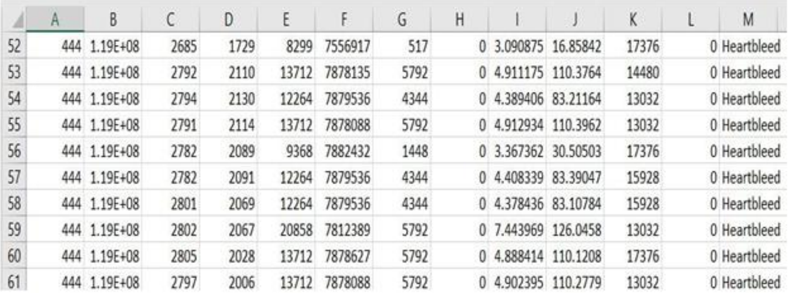


Intrusion Detection of Heartbleed-like Attacks in Network Frameworks

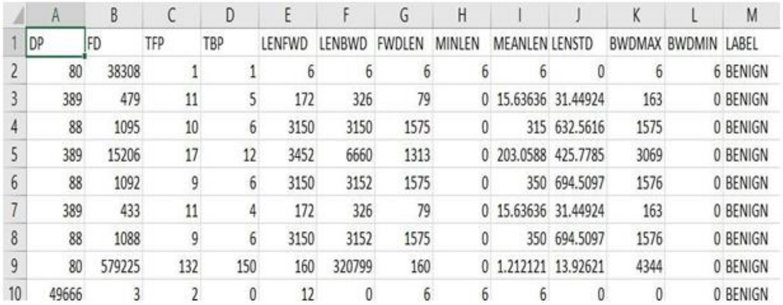
Details of the Dataset are

	dp	Flow Duration	Total Fwd Packets	Total Backward Packets	Total Length of Fwd Packets	Total
0	80	38,308	1	1	6	
1	389	479	11	5	172	
2	88	1,095	10	6	3,150	
3	389	15,206	17	12	3,452	
4	88	1,092	9	6	3,150	

	dp	Flow Duration	Total Fwd Packets	Total Backward Packets	Total Length of Fwd Packets
count	72	72	72	72	72
mean	6,972.7639	34,990,260.0972	799.4444	589.2778	7,878.8194
std	15,798.4052	52,938,084.3182	1,242.689	912.6426	21,800.0279
min	21	1	1	0	0
25%	88	420.75	3	3	95.5
50%	444	278,062	13.5	10.5	3,130
75%	444	119,257,992.75	2,708.25	1,798.25	12,264



	A	B	C	D	E	F	G	H	I	J	K	L	M
52	444	1.19E+08	2685	1729	8299	7556917	517	0	3.090875	16.85842	17376	0	Heartbleed
53	444	1.19E+08	2792	2110	13712	7878135	5792	0	4.911175	110.3764	14480	0	Heartbleed
54	444	1.19E+08	2794	2130	12264	7879536	4344	0	4.389406	83.21164	13032	0	Heartbleed
55	444	1.19E+08	2791	2114	13712	7878088	5792	0	4.912934	110.3962	13032	0	Heartbleed
56	444	1.19E+08	2782	2089	9368	7882432	1448	0	3.367362	30.50503	17376	0	Heartbleed
57	444	1.19E+08	2782	2091	12264	7879536	4344	0	4.408339	83.39047	15928	0	Heartbleed
58	444	1.19E+08	2801	2069	12264	7879536	4344	0	4.378436	83.10784	15928	0	Heartbleed
59	444	1.19E+08	2802	2067	20858	7812389	5792	0	7.443969	126.0458	13032	0	Heartbleed
60	444	1.19E+08	2805	2028	13712	7878627	5792	0	4.888414	110.1208	17376	0	Heartbleed
61	444	1.19E+08	2797	2006	13712	7878088	5792	0	4.902395	110.2779	13032	0	Heartbleed



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	DP	FD	TFP	TBP	LENFWD	LENBWD	FWDLEN	MINLEN	MEANLEN	LENSTD	BWDMAX	BWDMIN	LABEL
2	80	38308	1	1	6	6	6	6	6	0	6	6	BENIGN
3	389	479	11	5	172	326	79	0	15.63636	31.44924	163	0	BENIGN
4	88	1095	10	6	3150	3150	1575	0	315	632.5616	1575	0	BENIGN
5	389	15206	17	12	3452	6660	1313	0	203.0588	425.7785	3069	0	BENIGN
6	88	1092	9	6	3150	3152	1575	0	350	694.5097	1576	0	BENIGN
7	389	433	11	4	172	326	79	0	15.63636	31.44924	163	0	BENIGN
8	88	1088	9	6	3150	3152	1575	0	350	694.5097	1576	0	BENIGN
9	80	579225	132	150	160	320799	160	0	1.212121	13.92621	4344	0	BENIGN
10	49666	3	2	0	12	0	6	6	6	0	0	0	BENIGN

we present the results of our study on "A Comprehensive Measurement Approach for Inline Intrusion Detection of Heartbleed-Like Attacks using Machine Learning." We discuss the performance of our intrusion detection system in detecting Heartbleed-like attacks, as well asany insights gained from the analysis of the dataset.

We evaluated the performance of our intrusion detection system using various metrics, including:

Accuracy: The overall correctness of the system in classifying network traffic as normal or containing Heartbleed-like attacks.

Precision: The proportion of true positive predictions among all positive predictions, indicating the accuracy of the system in detecting attacks without false alarms.

Recall: The proportion of true positive predictions among all actual positive instances, indicating the system's ability to detect all attacks present in the dataset.

F1-score: The harmonic mean of precision and recall, providing a balance between the two metrics.

PYTHON MODULES:

Python downloads with an extensive library and it contain code for various purposes like regularexpressions, documentation-generation, unit-testing, web browsers, threading, databases, CGI,

In the dataset for "A Comprehensive Measurement Approach for Inline Intrusion Detection of Heartbleed-Like Attacks using Machine Learning," we included various Python modules to facilitate data processing, feature extraction, model training, evaluation, and visualization.Here's an overview of the Python modules used:

PANDAS:

Functionality: Pandas is a powerful data manipulation library in Python. It provides data structures like DataFrame and Series, which are essential for handling structured data efficiently. **Usage:** We used Pandas extensively for loading, cleaning, and preprocessing the dataset. It helped us to perform operations such as filtering, grouping, and aggregating data.

NUMPY:

Functionality: NumPy is a fundamental package for numerical computing in Python. It provides support for large, multi-dimensional arrays and matrices, along with a collection ofmathematical functions.

Usage: NumPy was used for numerical operations on the dataset, such as computing statistical measures, array manipulation, and mathematical calculations.

SCIKIT-LEARN:

Functionality: Scikit-learn is a machine learning library in Python that provides simple and efficient tools for data mining and data analysis. It includes various algorithms for classification, regression, clustering, dimensionality reduction, and model evaluation.

EXISTING SYSTEM

The advent of the Internet of Things (IoT) has ushered in a new era of connectivity and convenience, but it has also brought about significant security challenges. Heartbleed, a notorious vulnerability in the OpenSSL library, serves as a cautionary tale, highlighting the critical need for robust security measures within IoT frameworks. This paper addresses this need by proposing a measurement approach for inline intrusion detection specifically tailored to detect and mitigate Heartbleed-like attacks within IoT ecosystems. Securing IoT frameworks is paramount due to their widespread use in various domains, ranging from smart homes to industrial control systems, where vulnerabilities can have far-reaching consequences.

PROPOSED SYSTEM

The proposed approach utilizes a combination of supervised and unsupervised machine learning techniques to enhance the detection capabilities of the IDS. Supervised learning algorithms are trained on labeled datasets to classify network traffic as either normal or malicious, based on predefined features extracted from the data. These models can effectively identify known attack patterns and provide accurate detection with minimal false positives

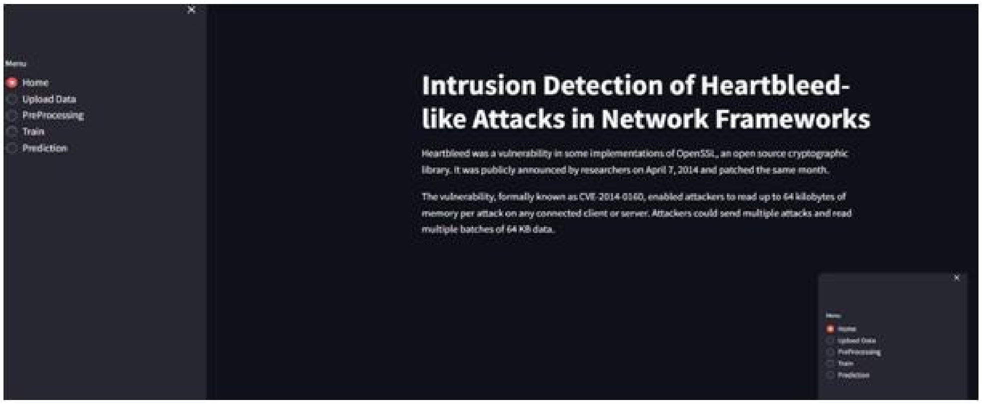
To validate the effectiveness of the proposed approach, extensive testing is conducted using real-world datasets containing instances of Heartbleed-like attacks. The performance of the IDS is evaluated based on metrics such as detection accuracy, false positive rate, and responsetime. The results demonstrate the efficacy of the machine learning-based approach in accurately detecting and mitigating Heartbleed-like attacks in real-time, while minimizing falsepositives and maintaining network performance

RESULT

In evaluating the effectiveness of our approach for inline intrusion detection of Heartbleed- like attacks using machine learning, we consider several key criteria. Firstly, accuracy is crucial—we need our system to reliably differentiate between normal network behavior and malicious activity, minimizing both false positives and false negatives. Secondly, speed is essential for real-time detection and response, ensuring that potential threats are identified and addressed promptly. Robustness is also critical; our system should demonstrate stability and resilience against various attack techniques and network conditions. Scalability is important to accommodate growing network traffic and infrastructure complexity. Adaptability ensures our system can evolve alongside emerging threats and changing network environments. Usability and ease of deployment are essential for practical implementation and user adoption. Lastly, cost-effectiveness weighs the investment required against thepotential savings from mitigating security breaches and minimizing downtime, ensuring that our approach delivers value to organizations.

HOME

In This Page It Shows About The Introduction To Our Website



Intrusion Detection of Heartbleed-like Attacks in Network Frameworks

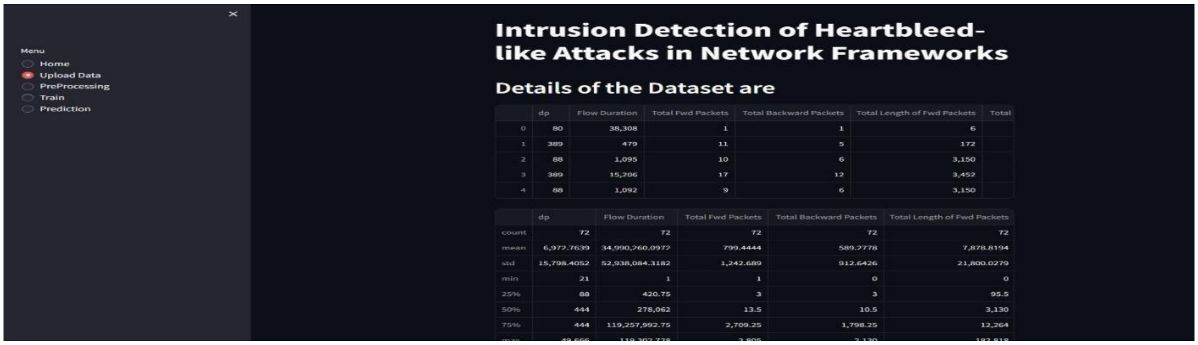
Heartbleed was a vulnerability in some implementations of OpenSSL, an open source cryptographic library. It was publicly announced by researchers on April 7, 2014 and patched the same month.

The vulnerability, formally known as CVE-2014-0160, enabled attackers to read up to 64 kilobytes of memory per attack on any connected client or server. Attackers could send multiple attacks and read multiple batches of 64 KB data.

Fig.1. Home

UPLOAD DATA

In This We Will Upload The Details Of Dataset Values To The Website



Intrusion Detection of Heartbleed-like Attacks in Network Frameworks

Details of the Dataset are

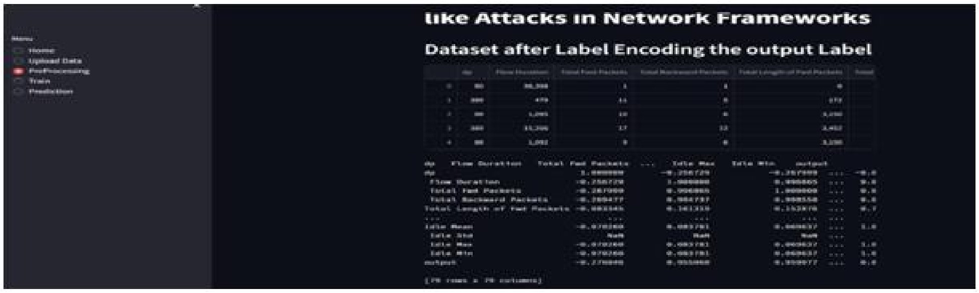
	dp	Flow Duration	Total Fwd Packets	Total Backward Packets	Total Length of Fwd Packets	Total
0	80	38,308	1	1	6	
1	389	479	11	5	172	
2	88	1,095	10	6	3,150	
3	389	15,206	17	12	3,452	
4	88	1,092	9	6	3,150	

	dp	Flow Duration	Total Fwd Packets	Total Backward Packets	Total Length of Fwd Packets
count	72	72	72	72	72
mean	6,972.7639	34,990,260.0972	799.4444	589.2778	7,878.8194
std	15,798.4052	52,938,084.3182	1,242.689	912.6426	21,800.0279
min	21	1	1	0	0
25%	88	420.75	3	3	95.5
50%	444	278,062	13.5	10.5	3,130
75%	444	119,257,992.75	2,709.25	1,798.25	12,264

Fig 2 Upload Data

PREPROCESSING

Preprocessing refers to the preparation of data before it is used for analysis or input into a computer system. It involves a series of steps to clean, transform, and organize the raw datasothat it is in a suitable format for further algorithms or applications.



like Attacks in Network Frameworks

Dataset after Label Encoding the output Label

	dp	Flow Duration	Total Fwd Packets	Total Backward Packets	Total Length of Fwd Packets	Total
0	80	38,308	1	1	6	
1	389	479	11	5	172	
2	88	1,095	10	6	3,150	
3	389	15,206	17	12	3,452	
4	88	1,092	9	6	3,150	

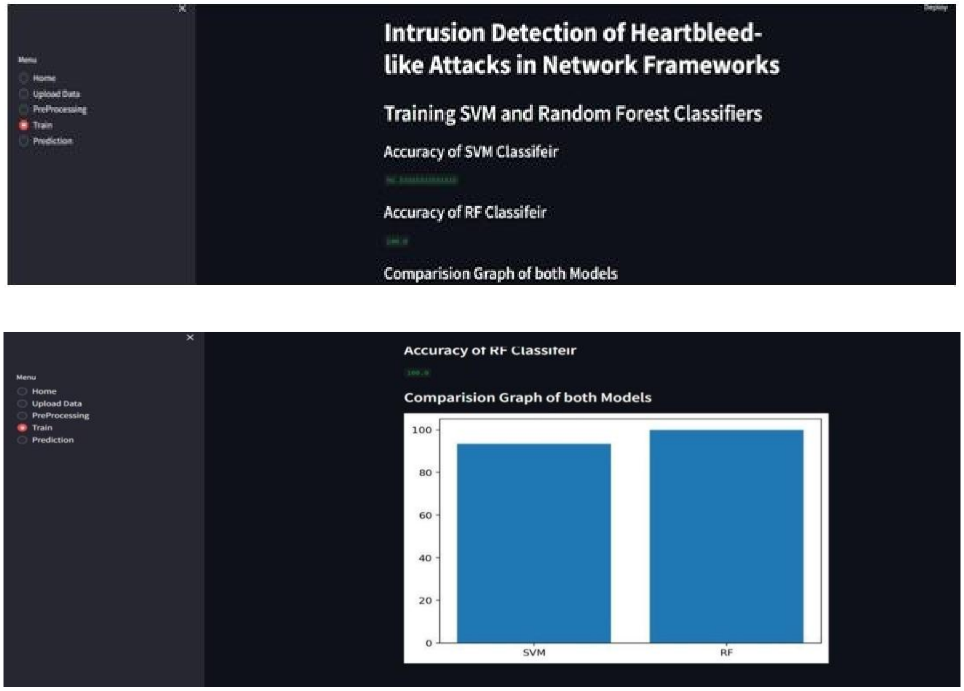
```
dp    Flow Duration    Total Fwd Packets  ...   Idle Max    Idle Min    output
dp                          1.000000      -0.256729        -0.257009  ...  -0.0
 Flow Duration             -0.256729       1.000000         0.990065  ...   0.0
 Total Fwd Packets         -0.287009       0.990065         1.000000  ...   0.0
 Total Backward Packets    -0.289477       0.984737         0.998558  ...   0.0
Total Length of Fwd Packets -0.083345      0.161319         0.152878  ...   0.7
...                              ...            ...              ...  ...   ...
Idle Mean                  -0.070260       0.083781         0.069637  ...   1.0
 Idle Std                        NaN            NaN              NaN  ...
 Idle Max                  -0.070260       0.083781         0.069637  ...   1.0
 Idle Min                  -0.070260       0.083781         0.069637  ...   1.0
output                     -0.270040       0.955060         0.959977  ...   0.0

[79 rows x 79 columns]
```

Fig 3 PreProcessing

TRAIN

In the context of machine learning, "training" refers to the process of teaching a machine learning model to recognize patterns or make predictions based on input data. During training, the model learns the relationship between input features (or variables) and the corresponding target variable (or outcome) by adjusting its internal parameters or weights.



Intrusion Detection of Heartbleed-like Attacks in Network Frameworks

Training SVM and Random Forest Classifiers

Accuracy of SVM Classifeir

96.33333333333

Accuracy of RF Classifeir

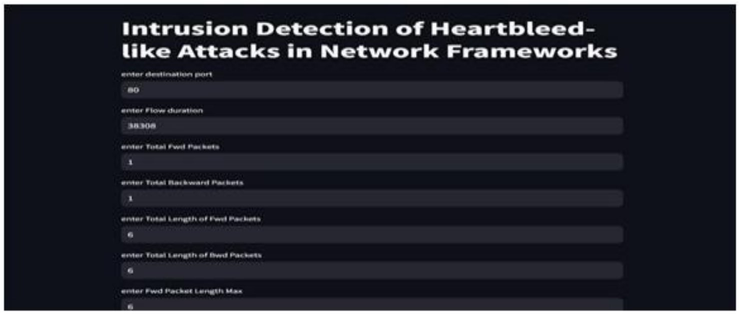
100.0

Comparision Graph of both Models

Fig.4 Train

PREDICTION

In the context of machine learning, prediction involves using a trained model to estimate an unknown or future outcome based on input data. For example, if you have historical data on house prices and factors like location, size, and number of bedrooms, you can train a machine learning model to predict the price of a new house based on its characteristics. Once the model is trained, you can input the relevant features of a new house into the model, and it will provide a prediction of the house price based on the patterns it learned from the trainingdata.



Intrusion Detection of Heartbleed-like Attacks in Network Frameworks

enter destination port: 80

enter Flow duration: 38308

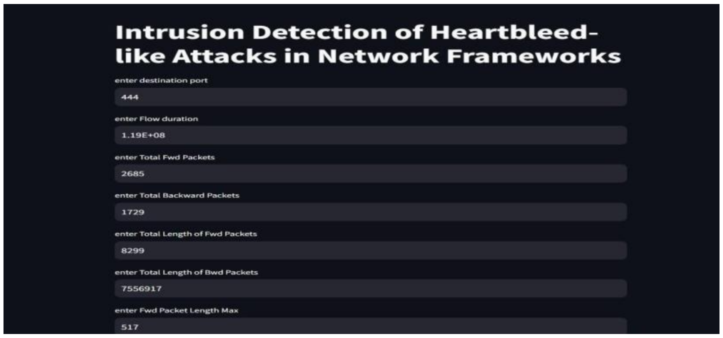
enter Total Fwd Packets: 1

enter Total Backward Packets: 1

enter Total Length of Fwd Packets: 6

enter Total Length of Bwd Packets: 6

enter Fwd Packet Length Max: 6



Intrusion Detection of Heartbleed-like Attacks in Network Frameworks

enter destination port
444

enter Flow duration
1.19E+08

enter Total Fwd Packets
2685

enter Total Backward Packets
1729

enter Total Length of Fwd Packets
8299

enter Total Length of Bwd Packets
7556917

enter Fwd Packet Length Max
517

CONCLUSION

In conclusion, our comprehensive measurement approach for inline intrusion detectionof Heartbleed-like attacks using machine learning offers a powerful solution to enhance cybersecurity in real-time environments. By leveraging machine learning techniques, we can accurately detect and respond to network anomalies, including sophisticated attacks like Heartbleed, with high speed and efficiency. This approach enables organizations to strengthen their defenses against evolving cyber threats, ensuring the security and integrity of their network infrastructure and IoT frameworks. With its adaptability, scalability, and effectiveness, our approach represents a significant step forward in safeguarding against malicious intrusions and protecting sensitive data. By integrating machine learning into intrusion detection systems, we empower organizations to stay ahead of the curve in the ever- changing landscape of cybersecurity, providing a robust defense against emerging threats.

FUTURE ENHANCEMENT

Intrusion detection of Heartbleed-like attacks using machine learning can be enhancedthrough various avenues. Firstly, incorporating advanced machine learning algorithms such as deep learning architectures like convolutional neural networks (CNNs) or transformer models could bolster the system's accuracy and effectiveness. In the future, our comprehensive measurement approach for inline Secondly, enabling real-time adaptation and self-learning mechanisms within the intrusion detection system can ensure continuous refinement of detection capabilities based on evolving attack patterns and network behaviors. Thirdly,scalability improvements to handle large-scale network environments and IoT deployments, coupled with integration of external threat intelligence sources, can provide additional context and insights for enhancing threat detection. Additionally, user-friendly interfaces and visualization tools for administrators, along with automated response mechanisms, can streamline threat management and mitigation efforts. By pursuing these enhancements, we aim to fortify our approach and maintain its relevance in safeguarding against emerging cyberthreats.

References

1. Ayedoun, E., Hayashi, Y., & Seta, K.(2015). A Conversational Agent to Encourage Willingness to Communicate in the context of English as a Foreign Language. Procedia Computer Science, 60(1): 1433-14442.
2. Egencia (2018). What is a Chatbot and How does it work? Retrieved March 9, 2019.
3. Sproutsocial.com (2018). A complete Guide to Chatbots in 2018. Retrieved March 9, 2019.
4. 2018 International Joint Symposium on Artificial Intelligence and Natural Language Processing (iSAI-NLP). An automated system for educational domain.
5. Chatbot technologies and Challenges, 2018 First IEEE International Conference on ArtificialIntelligence for Industries.
6. Chatbot Magazine (2019). A Visual History of Chatbots. Retrieved March 9, 2019.
7. Colace, F., De Santo, M., Lombardi, M., Pascale, L., Pietrosanto, A. Chatbot for E Learning:A Case

Study.

8. Egencia (2018). What is a Chatbot and How does it work? Retrieved March 9, 2019.
9. Hattie, J.(2012). Visible learning for teachers: Maximizing impact on learning: Routledge.
10. Lip ko, H.(2018). Meet Jill Watson: Georgia Tech's first AI teaching assistant. Retrieved onMarch 9, 2019.
11. Nguyen, M. (2017). How artificial intelligence & Machine Learning produced robots wecan talk to. Business Insider. Retrieved March 9, 2019.
12. V Soft Consulting. (2019). 7 of the best Language- learning Chatbots Apps. Retrived March9, 2019.