Journal of Al-Qadisiyah for Computer Science and Mathematics VOL.16(1) 2024, PP Comp. 21–31

Available online at www.qu.edu.iq/journalcm

JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS

ISSN:2521-3504(online) ISSN:2074-0204(print)

Detecting Brute Force Attacks on SSH and FTP Protocol Using Machine Learning: A Survey

***Amer Ali Hamza*[1], *Rana Jumma surayh Al-Janabi*[2]**

1College of Computer Science & Information Technology, University of Al-Qadisiyah, Al-Diwaniyah, Iraq.Email: amorali87@gmail.com

2College of Computer Science & Information Technology, University of Al-Qadisiyah, Al-Diwaniyah, Iraq.Email: Rana.aljanaby@edu.qu.iq

ARTICLE INFO

Article history:
Received: 6 /1/2024
Revised form: 5 /2/2024
Accepted: 21 /2/2024
Available online: 30 /3/2024

Keywords:

attack detection,

brute force attack,

FTP,

machine learning,

SSH.

ABSTRACT

The significance of detecting network traffic anomalies in cybersecurity cannot be overstated, especially given the increasing frequency and complexity of computer network attacks. As new Internet-related technologies emerge, so do more intricate attacks. One particularly daunting challenge is represented by dictionary-based brute-force attacks, which require effective real- time detection and mitigation methods. In this paper, we investigate Secure Shell or Secure Socket Shell, is a network protocol that gives users, particularly system administrators, a secure way to access a computer over an unsecured network(SSH)and File Transfer Protocol is a standard network protocol used for the transfer of files from one host to another over a TCP-based network, such as the Internet (FTP) brute-force attack detection by using Our research focuses on using the machine learning approach to detect SSH and FTP brute-force attacks. A reasonably thorough investigation of machine learners' efficacy in identifying brute force assaults on SSH and FTP is made possible by employing several classifiers. Brute-force assaults are a popular and risky method of obtaining usernames and passwords. Applying ethical hacking is an excellent technique to examine the effects of a brute-force assault. This article discusses many defense strategies and approaches to using brute-force assaults. The pros and cons of several defense strategies are enumerated, along with information on which kind of assault is easiest to identify. we made use of machine learning classifiers: Naive Bayes, Random Forest, Logistic Regression, we determined that the Random Forest algorithm achieved the highest level with an accuracy the contribution lies in demonstrating the feasibility of training and evaluating basic Random Forest models with two independent variables to classify CSE-CIC-IDS2018 dataset.

MSC.

https://doi.org/10.29304/jqcsm.2024.16.11432

∗Corresponding author: Amer Ali Hamza

Email addresses: amorali87@gmail.com

Communicated by:

1.Introduction

A brute force attack is a method where an attacker tries all possible Iterating through many combinations of passwords or encryption keys until the right one is discovered. It's a common method used to crack passwords. Due to the increasing dependency on digitalization, various security incidents, such as unauthorized access [1], Intrusion detection systems (IDS), firewalls, and antivirus software are just a few of the security measures available.[2]

The early warning system against network assaults of the IDS makes significant contributions. On high-speed networks, encrypted communication makes it difficult to identify these kinds of assaults at the network level. [3], The study provides a thorough evaluation of many machine learning methods utilized in computer security systems. [4] the researcher shows that just keeping an eye on the network may help us detect malicious activity like BFA. At the network level, identifying dictionary-based SSH and FTP brute-force assaults requires an efficient and high-performing technique.

Due to the large volume of data communications the majority of which are benign we must carefully examine the traffic flow data in order to identify malicious activity [5].

the attacker guessing list of usernames and passwords to get combinations to reach to the successful credential as shown in Fig.1[6].

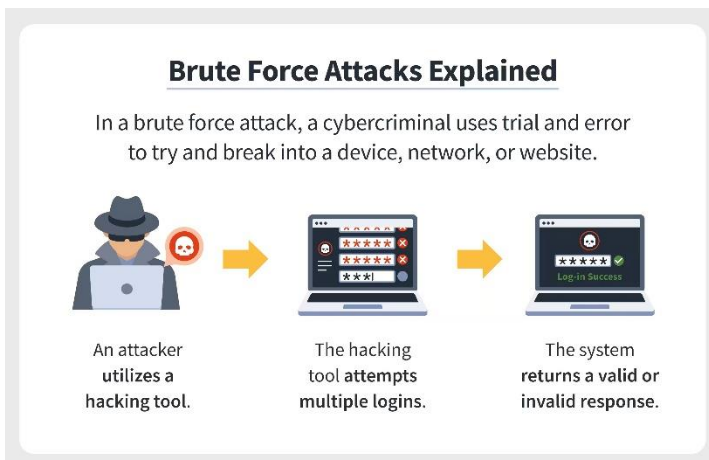

Fig. 1 Key steps of Brute Force Attack. [6]

During a dictionary attack, a hacker will use a dictionary file to attempt hundreds or possibly millionsof popular passwords one by one until they find the right one. A hacker may access a system and all of its data if they are successful in carrying out a dictionary attack., the Fig.2) shown how attackerusing dictionary attacks to get logon in a dictionary attack, the hacker tries a list of known or commonly used passwords. While a brute-force attack tries every character combination to break a password, a dictionary attack only attempts passwords previously leaked or commonly used by others.[7].

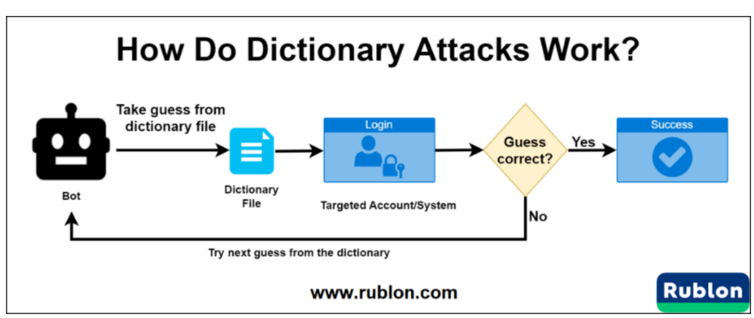

Fig. 2 Work architecture of Dictionary Brute Force Attack.[7]

The study the performance of Detection of SSH and FTP brute-force attacks, together with the classifiers' classification accuracy.

The contribution to this is collecting previous work and identifying the benefits and harms of each research project, the strengthsand weaknesses, the methods used, including algorithms and others, the accuracy of each classifier, and the type of data set used for the last five years, and then presenting the method used in my research,which is a very modern method that will achieve very high results.

Therefore, in this paper, propose a Machine Learning model for detecting brute-force attacks on FTP and SSH protocols. Brute-force attacks targeting these protocols have become increasingly significant security risks to organizations. By leveraging the capabilities of Machine Learning, the model aims to overcome the limitations of traditional IDSes and improve the accuracy and efficiency of brute-force attack detection on FTP and SSH protocols. Through an extensive evaluation and comparison with existing literature, our findings demonstrate that the proposed model achieves high accuracy outperforming other comparable solutions in detecting brute- force attacks.

1. Algorithms and Techniques

This section gives brief overviews of the three ML algorithms used in this work and their graphical presentations

2.1 Random Forest (RF)

The random forest (RF) method is comprised of several decision trees. Every one of these trees produces a forecast. Subsequently, the algorithm utilizes these predictions to formulate a judgment by considering the majority of the expected values. RF has many benefits, including as its versatility in solving both classification and regression issues, its independence from scaling requirements, and its capability to effectively manage outliers. The approach has many drawbacks, such as its high processing requirements due to the involvement of numerous decision trees, resulting in lengthier training times for models. as shown in Fig.3.

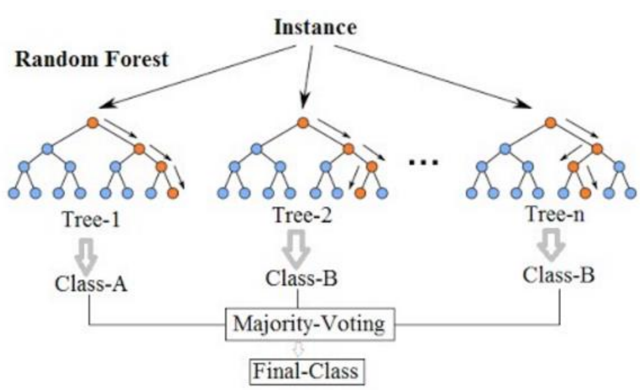

Fig. 3 Random Forest (RF)

2.1.2 Gaussian Naive Bayes (NB)

Bayesian classifiers are statistical classifiers. They may predict the likelihood that the supplied model is suitable for a certain class. Gaussian Naive Bayes (GNB) is a variant of the Naïve Bayes algorithm that utilizes Bayes's theorem. The underlying assumption of these algorithms is that, within a certain class, the attribute value is unrelated to the values of other attributes. The name given to this theory is class-conditional independence. It is mostly used for datasets containing continuous data. This approach presupposes that classes adhere to a Gaussian distribution.

The Gaussian distribution, often known as the normal distribution, may be examined using the following formula. Some of the benefits of utilizing GNB include that it is a rapid technique to train, is good for datasets with numerous classes, and is typically used for categorical issues.

An inherent drawback of this approach is its tendency to consider each characteristic in isolation, a scenario that does not necessarily reflect real-world conditions. This renders the algorithm less applicable to real-world scenarios. as shown in Fig.4)

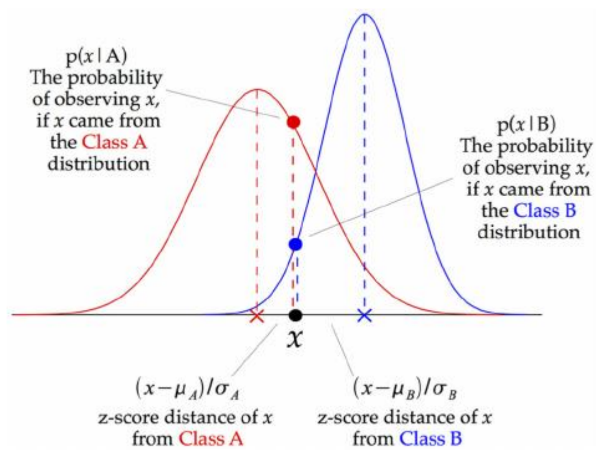

Fig. 4 Gaussian Naive Bayes (GNB)

2.1.3 Logistic Regression (LR)

Logistic regression (LR) is a statistical technique used for binary classification, which estimates the chance of an event occurring by using a probability function. The probability is calculated using the following formula. Some benefits of this method include its ability to quickly classify data and its ease of extension to handle multi-class problems. An inherent limitation of LR is its inability to address nonlinear problems. as shown in Fig.5.

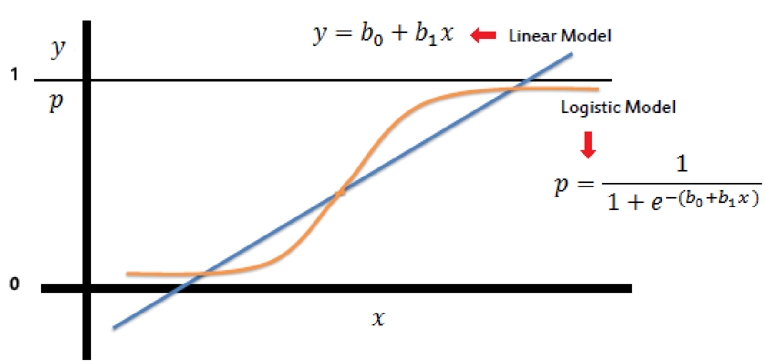

Fig.5 Logistic Regression (LR)

2. Types of Brute Force Attack (BFA)

Each brute-force attack might utilize a variety of tactics to unearth confidential information. Any of the following common brute force techniques could be used against the intended victim:

1) Basic Traditional Brute Force Attack: This is a basic kind of brute force attack in which a hacker is given a username or list of usernames and tries to guess passwords until the right combination is discovered, either manually or by using a brute force programming script.

2) Reverse Brute Force Attacks: This technique involves a hacker using a known password, either via a breach or regularly used, and systematically trying several usernames until a successful combination is discovered. These attacks vary from standard brute force or dictionary attacks in that they operate in reverse, beginning with known passwords rather than known users.

3) Dictionary Attacks: A sophisticated technique in which a hacker uses a precompiled list of terms derived from extensive study on the target or tiny modifications of commonly used (or possible) passwords, in order to systematically test them against a given login. The selected list is regarded as a "lexicon" of modified or slightly modified words or character combinations.

4) Hybrid assaults refer to the technique of merging classic brute force assaults with dictionary attacks. The hacker employs a technique known as dictionary attack, where they extract the most frequently used phrases and words from a predefined "dictionary" and systematically generate several password permutations until they successfully discover the correct combination.

5) Credential Stuffing refers to a technique in which a hacker exploits a known set of login and password combinations to gain unauthorized access to additional accounts, profiles, or systems linked to the same user. This attack is successful because to the common practice of individuals reusing passwords across many accounts.

3.1 Detection and prevention of brute force attacks on FTP and SSH protocols:

- Account lockout: Enforce a protocol that automatically restricts user accounts after a certain threshold of unsuccessful login attempts. This may aid in mitigating brute-force assaults.
- Intrusion detection systems (IDS): Use an IDS to monitor network traffic and detect any unusual or repetitive patterns that may indicate a brute force attack in progress. IDS can analyze traffic and identify multiple failed logins attempts from a single or multiple IP addresses.
- Two-factor authentication (2FA): Enforce the use of 2FA for FTP and SSH logins. This enhances security by requiring an additional piece of information to be provided. such as a one-time password or biometric verification, in addition to the regular login credentials.
- IP blocking: Track repeated failed login attempts from specific IP addresses and automatically block them after a certain threshold is reached. This can be done at the firewall or server level.
- Log monitoring and analysis: Regularly monitor the logs of your FTP and SSH servers for suspicious login attempts and analyze patterns to identify potential threats. This can help you proactively detect and respond to brute-force attacks.
- Enforce rate-limiting: Deploy methods that limit the number of login attempts allowed within a certain period of time. This can help prevent automated attacks that attempt to deduce passwords by imposing restrictions on the number of permissible trials.
- Use strong and inimitable passwords.
- Use Web application firewalls (WAFS).
- Employ a CAPTCHA.

3. Related works

Many academic papers have been written to propose solutions for reducing BFA attacks. However, despite the vast amount of academic research, BFA attacks continue to be widespread, especially when it comes to SSH and FTP attacks. Despite this, we will now present a summary of the most significant studies on these types of attacks to emphasis The significance of our job.

In the paper [8], John Hancock et al., The issue of brute force assaults in large data and the research on Big Data illustrates the viability of using simple decision tree models with two independent variables to precisely classify SSH and FTP brute force assaults. with dataset CSE-CIC-IDS2018 Accuracy% 0.99, are capable of detecting.

In the paper [9], Stiawan et al. Investigated a methodology for systematically testing various attack patterns in an Internet of Things (IoT) network environment. The brute-force assault was successfully identified.

In the paper [10], Najafabadi et al. Conducted an investigation on detecting Network-level SSH brute-force attacks may be detected by analysing NetFlow data. A dataset specifically designed for attack detection was generated, using machine learning techniques that have shown effectiveness in recognising brute-force attacks. The researchers investigated distributed SSH brute-force attacks and evaluated an 8-year login dataset including many users. It has been shown that some individual attack detection methods provide difficulties in terms of implementation.

In the paper [11], Satoh et al. The researchers conducted an analysis of SSH dictionary attack detection using machine learning. Subsequently, they included two innovative components for detecting such attacks.

In the paper [12], Kahara Wanjau et al. The research presents a very effective approach for detecting SSH-brute force network attacks using a supervised deep learning method called Convolutional Neural Network (CNN). The CNN-based model outperforms existing machine learning approaches in detecting SSH brute force assaults. It has an F1-score of 91.8%, an accuracy rate of 94.3%, An accuracy rate of 92.5% and a recall rate of 97.8% were achieved. The model was tested with the CIC-IDS 2018 dataset, which was pre-processed by converting raw data into images for training and testing. The study results demonstrate that deep neural networks (DNN) exhibit superior performance compared to other intrusion detection systems based on machine learning. The proposed method in the study combines feature selection and a deeplearning algorithm for SSH-brute force attack detection.

In paper [13], Stephen Kahara Wanjau et al. Based on the Convolutional Neural Network, a supervised deep learning algorithm, this paper suggests a good way to find SSH brute force network attacks. The model's performance was compared to the outcomes of five well-known Machine learning techniques The mentioned machine learning algorithms include Naive Bayes, Logistic Regression, Decision Tree, k-Nearest Neighbour, and Support Vector Machine. Four often used metrics, namely accuracy, precision, recall, and the F-measure, were utilised. Our investigation revealed that the CNN-based model outperforms conventional machine learning techniques in detecting SSH brute force assaults. The F1-score was 91.8%, the accuracy rate was 94.3%, the precision rate was 92.5%, and the recall rate was 97.8%.

In paper [14], Liang Zhou et al. Suggest an innovative methodology that leverages Machine learning techniques are used to assist in the classification of cyberattacks. created a deep neural network (DNN) model and carefully determined the appropriate global parameters to attain outstanding generalization performance. The evaluation result demonstrates that the proposed methodology can effectively identify cyber-attacks in smart grids, with an accuracy rate of up to 96%.

In paper [15] by M. D. Hossain et al., The assaults occur the user's text is empty. Dictionary-based brute-force attacks (BFA) are prevalent forms of sophisticated cyber-attacks. The researcher investigates the identification of SSH and FTP brute-force assaults using the use of the Long Short-Term Memory (LSTM) deep learning technology. Furthermore, we used machine learning classifiers such as J48, naive Bayes, decision table, random forest, and k-nearest neighbour to augment our detection capabilities. We used the highly esteemed annotated dataset CICIDS2017. they evaluated the effectiveness of the LSTM and ML algorithms and performed a comparative study of their performance. The results suggest that the LSTM model outperforms the ML algorithms in terms of performance. achieving a precision level of 99.88%.

In a paper [16] by Noura Alotibi et al., There has been an increase in the occurrence of brute-force assaults that specifically target FTP and SSH protocols. As a reaction, researcher provide a new and clever method that relies Utilising a dataset, the focus is on employing deep learning techniques to detect and classify brute-force attacks on FTP and SSH protocols. The CSE-CIC-IDS2018 approach achieves a remarkable accuracy rate of 99.9%, surpassing previous comparable approaches in identifying brute-force attacks. The model architecture used was LSTM combined with the SMOTE method, resulting accuracy 96.2.

In the paper [17], by Shailesh Singh Panwar et al., The primary emphasis is on seven distinct approaches, such as the brute force attack, achieved via the use of diverse Algorithms that pick features based on subsets. The execution assaults have occurred determined regarding several aspects. The use of these methodologies has led to the identification of the optimal set of qualities for detecting all types of attacks, using relevant classification algorithms. The efficacy of Intrusion Detection Systems (IDS). Performance assessment of brute force assaults using the classifier with a 90% accuracy rate and the CICIDS-2017 dataset for intrusion detection employing WEKA.

In paper [18], Karel Hynek et al. Suggest an innovative method for identifying SSH brute-force assaults on high-speed networks. Instead, then using host-based methods, approach focuses on analyzing network traces to detect and identify intruders.

the existing resolution. In order to address the problem of elevated false positive rates, we suggest using a machine learning (ML) technique for detection that utilizes specifically expanded IP flows. Recent publications detail the methodology of accurately identifying BF assaults using just NetFlow data, achieving a high level of precision and a low percentage of false positives. Additionally, these articles discuss the structure and design of the detection system. The training dataset was constructed by meticulously examining actual traffic that was recorded, authentic SSH traffic that was manually manipulated to resemble brute force assaults, and ultimately a packet path including Logs of SSH activity from authentic production servers.

In a paper [19] by Joffrey L. Leevy et al., there has been a rise in cyberattacks to match the rapid expansion of computer networks and network applications on a global scale. The survey studies the conducted has yielded some significant conclusions. Upon analysis, they found that the performance ratings for each research, when accessible, exhibited unusually high levels of achievement. This phenomenon might perhaps be attributed to the overfitting of large data studies. Furthermore, they found that the documentation about the data cleaning process of CSECIC-IDS2018 was insufficient in all areas, suggesting potential issues with the replicability of studies. the survey has also found significant research deficiencies.

In the paper [20] by Stephen Kahara Wanjau et al., Brute force assaults are a prominent kind of network attack that presents significant dangers to network security. To stop in order to prevent the recurrence of such assaults, it is necessary to implement certain remedial measures. This research proposes an effective method for detecting SSH brute-force network assaults using a supervised deep learning methodology, namely a convolutional neural network, and a machine learning algorithm. The machine learning methods mentioned include (NB), LR, DT, k-NN and Support SVM, with 94.3%.

in paper [21] According to Maryam M. Najafabadi et al., A brute force assault is a very common network attack that poses a significant danger to machines linked to the network. This study examines the use of machine learning techniques to identify brute force attacks on the SSH protocol at the network level.

in paper [22] Deris Stiawan et al. The File Transfer Protocol (FTP) server located at a data sink or gateway is frequently configured incorrectly. Simultaneously, password cracking and theft are prevalent methods used by attackers to target The Internet of Things (IoT) network. This study aims to provide a deeper understanding into this specific kind of assault, with the primary objective of identifying Possible assault strategies assist the administrator of the Internet of Things (IoT) system in analyzing Comparable assaults. This study examines Brute force attacks (BFA) targeting the FTP server of the Internet of Things (IoT) network. It employs a temporally dependent statistical correlation technique to analyze and visualize the assault patterns that were observed may be identified.
Table 1 and Table 2 display supervised algorithms, as well as autoencoder and deep belief network architectures used for SSH and FTP brute force Attacks Detection, respectively.

Table 1. Comparison of SSH and FTP brute force Attacks Detection Schemes using ANN and CNN Architectures

Scheme	Data used	Model architecture	Result in %
[23]	CICIDS 2017, UNSW-NB15, NSL-KDD, Kyoto, WSN-DS	ANN + ReLU activation	Accuracy: 78.5 Precision: 81 Recall: 78.5 F1- score: 76.5
[24]	ISCX VPN	CNN	Accuracy: 99.85
[25]	NSL-KDD	ANN + ReLU activation	Accuracy: 86.35, Precision: 81.86, Recall:77.32, F1-score: 73.89, FAR: 0.1619
[26]	KDD 99	ANN + ReLU activation	Accuracy: 99.01, Recall:99.81, FAR: 0.0047
[27]	Network data Simulated by IoT	ANN + Sigmoid activation	Accuracy: 99

Table 2. Comparison of SSH and FTP brute force Attacks LSTM RNN and Other Deep Learning Architectures

Scheme	Data used	Model Architecture	Result in %
[28]	NSL-KDD, binary and 5-class classification	RNN	Accuracy: 81.29
[29]	KDD 99	LSTM network	Accuracy: 97.54, Precision: 97.69, Recall:98.95, FAR: 9.98
[30]	CSE-CIC- IDS2018	Broad Learning System	Accuracy: 97.08 F1- score: 77.89 Precision: NA Recall: NA
[31]	CSE-CIC- IDS2018	LSTM+ SMOTE algorithm	Accuracy :96.2 F1- score: NA Precision :96 Recall :96
[32]	CSE-CIC- IDS2018	Spark ML + Conv-AE	Accuracy: 98.20 F1- score: 98 Precision: NA Recall :98

4. Methodology

The methodology section outlines the process followed in developing the Brute Force attack on SSH and FTP protocol detection model using Machine Learning techniques. The chosen algorithm is based on the CSE-CIC-IDS 2018 dataset, specifically the FTP/SSH brute-force attacks, serve as the basis for the model. The entire process is broken down into distinct stages, as detailed below:

1) Obtain the proposed benchmark dataset: The CSE-CIC- IDS 2018 dataset is acquired, containing eight different attack types. Only FTP/SSH brute-force attacks are used in this study.

2) Prepare the data: Data preprocessing involves correcting issues such as missing values and outliers, ensuring that the dataset is clean and ready for analysis.

3) Use exploratory analysis: This step involves understanding the dataset's content and selecting the most suitable algorithm for the given problem.

4) Train the model: The best-performing algorithm from the literature review is used to train the model on the prepared dataset.

5) Evaluate the model: Evaluation techniques are employed to assess the model's performance and ensure that it meets the desired accuracy and detection standards.

6) Optimize the model: If the model's performance is unsatisfactory, alternative algorithms are considered or the current model's parameters are adjusted to improve its effectiveness.

5.1 Dataset:

use data set CSE-CIC-IDS2018 in our search The Communications Security Establishment (CSE) and the Canadian Institute for Cybersecurity (CIC) developed the CSE-CIC-IDS2018 dataset to meet the needs of the attack detection benchmark dataset that represents traffic composition and attack on the current modern network This dataset consists of 80 features, including labels. The dataset is collected from Amazon´s AWS LAN network It includes seven different attack classes features extracted from the captured traffic using CICFlowMeter-V3.

The output of the application is in CSV file format with six columns labeled for each flow, namely FlowID, SourceIP, DestinationIP, SourcePort, DestinationPort, and Protocol with more than 80 network traffic features.

6. Discussion

Based on the assessment findings, machine learning algorithms exhibited a high level of accuracy. However, this is due to the fact that the number of benign occurrences in the dataset is larger than the number of instances of SSH and FTP assaults. Therefore, In the performance analysis, we evaluated precision, recall, F1-score, and AUC-ROC. During the confusion matrix analysis, we noted that the overall weighted classifier accuracy, precision, recall, and F1-score were all high. The F1-score should be increased. When it comes to deploying these types of models in real-time settings. Based on the AUC-ROC curve, we saw that the area under the curve approached 1.0, indicating strong evidence that (RF) model is effective in identifying FTP and SSH brute-force assaults. The (RF) Intrusion Detection System (IDS) we present is very efficient in identifying and detecting FTP and SSH brute-force assaults on network systems.

It is feasible to deploy a model in real-time to identify brute force assaults. The performance of (RF) was subpar in our observations. To identify web brute-force assaults. Our next study will focus on enhancing the detection rate and F1-score of these assaults by using other deep learning models

7.Conclusion and Future Work:

In this paper we proposed efficient strategies to promptly identify and counteract such brute-force assaults instantaneously. Multiple machine learning (ML) classifiers are used to analyze and identify Secure Shell (SSH) and File Transfer Protocol (FTP) brute-force assault Identification. The following machine learning algorithms include Naive Bayes (NB), Random Forest (RF), Logistic Regression (LG),

The objective of detecting brute-force attacks is to identify and prevent unauthorized intrusion into computer systems or networks via the process of detection repeated, rapid attempts to guess passwords or encryptionkeys. By detecting these types of attacks, security measures can be implemented to block or minimizethe impact of such malicious activities, safeguarding data and ensuring system integrity. This paper Provides a thorough examination of the many methods used in carrying out brute-force assaults.

along with recommendations for safeguarding oneself against such attacks. It becomes evident that a combination of multiple protective measures is imperative, thereby enhancing security. It has been demonstrated that the execution of a brute-force attack is comparatively straightforward yet highly extensive, resulting in considerable harm to the targeted users. The benefits and drawbacks of distinct protective mechanisms are underscored, facilitating users in selecting the most appropriate combination of protection methods.

End users should adopt brute-force attack defense strategies on awidespread basis because they have proven to be incredibly effective in real-world situations. Future endeavors will concentrate on monitoring novel brute-force attack methodologies and conducting vulnerability analyses of targeted systems while adhering to the principles of ethical hacking to identifyoptimal defense strategies. Comparison of our model's results with various evaluation metrics reveals its superior ability to detect brute-force attacks, outperforming other recent research studies. The key metrics obtained are high accuracy, and F1-score, and precision, and recall.

Future work could focus on refining the artificial neural network model and comparing its performance with other machine learning models, such as Support Vector Machines (SVM), decision trees, and These comparisons would provide valuable insights into the model's performance and potential for further enhancement. Additionally, future research may explore the applicability of the proposed model to a wider range of cyberattacks.

References

[1] H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," J Big Data, vol. 7, pp. 1–29, 2020.

[2] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, "A survey of network-based intrusion detection data sets," Comput Secur, vol. 86, pp. 147–167, 2019.

[3] K. Kim, M. E. Aminanto, and H. C. Tanuwidjaja, Network intrusion detection using deep learning: a feature learning approach. Springer, 2018.

[4] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, "On the effectiveness of machine and deep learning for cyber security," in 2018 10th international conference on cyber Conflict (CyCon), IEEE, 2018, pp 371–390.

[5] N. Bakhareva, A. Shukhman, A. Matveev, P. Polezhaev, Y. Ushakov, and L. Legashev, "Attack detection in enterprise networks by machine learning methods," in 2019 international Russian automation conference (RusAutoCon), IEEE, 2019, pp. 1–6.

[6] https://www.spiceworks.com/it-security/cyber-risk-management/articles/what-is-brute-force-attack/

[7] https://rublon.com/blog/brute-force-dictionary-attack-difference/

[8] J. Hancock, T. M. Khoshgoftaar, and J. L. Leevy, "Detecting SSH and FTP Brute Force Attacks in Big Data," in Proceedings - 20th IEEE International Conference on Machine Learning and Applications, ICMLA 2021, Institute of Electrical and Electronics Engineers Inc.,2021, pp. 760–765. doi: 10.1109/ICMLA52953.2021.00126.

[9] D. Stiawan, M. Idris, R. F. Malik, S. Nurmaini, N. Alsharif, and R. Budiarto, "Investigating brute force attack patterns in IoT network," Journal of Electrical and Computer Engineering, vol. 2019, 2019.

[10] M. M. Najafabadi, T. M. Khoshgoftaar, C. Kemp, N. Seliya, and R. Zuech, "Machine learning for detecting brute force attacks at the network level," in 2014 IEEE International Conference on Bioinformatics and Bioengineering, IEEE2014, pp. 379–385.,

[11] A. Satoh, Y. Nakamura, and T. Ikenaga, "SSH dictionary attack detection based on flow analysis," in 2012 IEEE/IPSJ 12th International Symposium on Applications and the Internet, IEEE, 2012, pp.

[12] S. Kahara Wanjau, G. M. Wambugu, and G. Ndung'u Kamau, "SSH-Brute Force Attack Detection Model based on Deep Learning," 2021. [Online]. Available: www.ijcat.com.

[13] S. K. Wanjau, G. M. Wambugu, and G. N. Kamau, "SSH-brute force attack detection model based on deep learning," 2021.

[14] L. Zhou, X. Ouyang, H. Ying, L. Han, Y. Cheng, and T. Zhang, "Cyber-attack classification in smart grid via deep neural network," in Proceedings of the 2nd international conference on computer science and application engineering, 2018, pp. 1–5

[15] . M. D. Hossain, H. Ochiai, F. Doudou, and Y. Kadobayashi, "ssh and ftp brute-force attacks detection in computer networks: Lstm and machine learning approaches," in 2020 5th international conference on computer and communication systems (ICCCS), IEEE, 2020, pp. 491–497.

[16] N. Alotibi and M. Alshammari, "Deep Learning-based Intrusion Detection: A Novel Approach for Identifying Brute-Force .

[17] Panwar, S. S., Negi, P. S., Panwar, L. S., & Raiwani, Y. P. (2019). Implementation of machine learning algorithms on cicids-2017 dataset for intrusion detection using WEKA. International Journal of Recent Technology and Engineering, 8(3), 2195–2207.

[18] Hynek, K., Beneš, T., Čejka, T., & Kubátová, H. (2020). Refined detection of SSH brute-force attackers using machine learning. ICT Systems Security and Privacy Protection: 35th IFIP TC 11 International Conference, SEC 2020,Maribor, Slovenia, September 21–23, 2020, Proceedings 35, 49–63.

[19] J. L. Leevy and T. M. Khoshgoftaar, “A survey and analysis of intrusion detection models based on CSE-CIC-IDS2018 Big Data. J. Big Data 7, 104 (2020).”

[20] S. Kahara Wanjau, G. M. Wambugu, and G. Ndung’u Kamau, “SSH-Brute Force Attack Detection Model based on Deep Learning,” 2021. [Online]. Available: www.ijcat.com.

[21] M. M. Najafabadi, T. M. Khoshgoftaar, C. Kemp, N. Seliya, and R. Zuech, “Machine learning for detecting brute force attacks at the network level,” in 2014 IEEE International Conference on Bioinformatics and Bioengineering,IEEE, 2014, pp. 379–385.

[22] D. Stiawan, M. Idris, R. F. Malik, S. Nurmaini, N. Alsharif, and R. Budiarto, “Investigating brute force attack patterns in IoT network,” Journal of Electrical and Computer Engineering, vol. 2019,2019.

[23] R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, A. Al- Nemrat, and S. Venkatraman, „Deep learning approach for intelligent intrusion detection system‟, Ieee Access, vol. 7, pp. 41525–41550, 2019.

[24] Y. Zeng, H. Gu, W. Wei, and Y. Guo, „$ Deep-Full-Range $: a deep learning based network encrypted traffic classification and intrusion detection framework‟, IEEE Access, vol. 7, pp. 45182–45190, 2019.

[25] W. Wang et al., „HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection‟, IEEE access, vol. 6, pp. 1792–1806, 2017.

[26] X. Jin, J. Zhou, H. Dong, W. Lou, J. Wang, and F. Wang, „Research on new military plotting system architecture based on AutoCAD secondary development‟, 2017, pp. 313–317.

[27] E. Hodo et al., „Threat analysis of IoT networks using artificial neural network intrusion detection system‟, 2016, pp. 1–6.

[28] C. Yin, Y. Zhu, J. Fei, and X. He, „A deep learning approach for intrusion detection using recurrent neural networks‟, Ieee Access, vol. 5,pp. 21954–21961, 2017.

[29] T. H. T. Le, N. H. Tran, P. L. Vo, Z. Han, M. Bennis, and C. S. Hong„„Contract-based cache partitioning and pricing mechanism in wireless network slicing‟, 2017, pp. 1–6.

[30] A. L. G. Rios, Z. Li, K. Bekshentayeva, and L. Trajković, „Detection of denial of service attacks in communication networks‟, 2020, pp. 1–5.

[31] P. Lin, K. Ye, and C.-Z. Xu, „Dynamic network anomaly detection system by using deep learning techniques‟, 2019, pp. 161–176.

[32] M. A. Khan and J. Kim, “Toward developing efficient Conv-AE-based intrusion detection system using heterogeneous dataset,” Electronics, vol. 9, no. 11, p. 1771, 2020.‟.