International Journal of Scientific Research and Engineering Development-– Volume 5 Issue 5, Sep- Oct 2022
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Cyber Security Readiness in Malawi

Eric Kalea[1st], Dr T. Samraj Lawrence [2nd], Dr G.Gloindal[3rd]
Student in Masters, DMI-St.Eugene University,Zambia,
ekalea@hotmail.com
Associate Professor Dambi Dollo University
samraj@dadu.edu.et
Head of Department, DMI-St.Eugene University,Zambia
pg@dmiseu.edu.zm

Abstract:

Illegal access to sensitive information, such as medical records, financial records, personal information, or other types of data that may negatively impact the business. Cybersecurity has become a serious threat to organizations that are not prepared or able to respond to cyberattacks. In Malawi, many organizations lack Management support and lack of Computer Emergency Response Teams. This paper presents a cyber-security culture framework for assessing and evaluating the current security readiness of an organizations. Every organization has the right to be protected and have good security protocols. With the latest's trends in technology, attackers are finding new ways to hack and compromise computer systems. Cyber security is essential for any business both corporate and non-corporate. Cyber security readiness is found to positively impact security performance, which in turn positively affects financial and non-financial performance. In addition to implementing basic cybersecurity controls like firewalls, intrusion detection, and VPNs, take steps to ensure your employees (end users) understand their role as they are the first line of defence. Cyber awareness training program to educate users on best practices. Reinforce the need for password hygiene (63% of data breaches result from weak or stolen passwords), frequent patch management. About 91% cyber-attacks are phishing emails, social engineering attacks, Ransomware attacks, and IPS Attacks end users and security teams need to be trained to handle such threats. The proposed computer-based emergency response teams can be used to orient and improve the current understanding of how organizations in Malawi can better equip themselves to minimize the occurrence and impact of cyber-attacks.

Keywords **—Intrusion Detection System(IDS); Firewall; Cyber Attack; Phishing; Decision Tree.**

----------**********----------

INTRODUCTION

In this digital age, Cybersecurity is the practice of protecting systems or networks, and programs from digital attacks and various cyber threats. News of cyber-attacks has become relatively common and is aimed at accessing, changing, or destroying sensitive information. Computer security is the ability to protect a computer system and its resources in reference to Confidentiality, Integrity, and Availability. To prevent cyber threats, various protocols and firewalls are used. Confidentiality requires that information can only be accessed by those who are authorized to access it; integrity requires that the information remain unchanged.Cyber security Readiness provides benefits for companies to detect and effectively respond to cyber threats, intrusions, breaches, malware attacks and phishing attacks.However, before an organization can have cyber security in place, it must be aware of the possibility of Hackers can perform different types of attacks in several ways which can lead in the theft of confidential data that can cripple the business, resulting in loss of revenue and damage to reputation to the company as well as leakage of sensitive information processes. Security response teams must be committed to preventing, Unauthorized intrusion, detecting, and combatting cyber-attacks. Intrusion prevention techniques, such as user authentication and authorization, encryption, and defensive programming, intrusion detection is often used as another wall to protect computer systems. In every company cybersecurity can improve its cyber defence and reputation and facilitate its core competency and superior organizational performance by being ready to respond to attacks.

 ©IJSRED: All Rights are Reserved

I. LITERATURE REVIEW

To ensure and enhance cyber resilience, the incident response mechanism must be effective. The effectiveness of modern emergency management relies on the uninterrupted operation of a range of information and communication systems. In this paper an endeavor is made to identify weak areas regarding the cyber resilience mechanism existing in Bangladesh. Critical Information Infrastructure Protection

End user Awareness Education and Personnel Training is highly required.

The effectiveness of modern emergency management relies on the uninterrupted operation of a range of information and communication systems [1].

According to Nikos Benias, Angelos P. Markopoulos companies need we need to understand how the system works and make it stronger and to train end users on how to practice safe internet habits [2].

According to Zakir Hossain, Golam Kibria Zaman and Kazi Abu Taher Computer Incident Response Team to mitigate the incident as soon as possible is to minimize the loss of data and resources. High-impact security threats, vulnerabilities and alert had to be analyzed. Threats need to be detected and respond in a timely all vulnerabilities need to be patched in a timely manner [3]. According to Shaikha Hasan, Mazen Ali, Sherah Kurnia Ramayah Thurasamy Develop a cyber security readiness frame which will top management support and understand the affecting cyber security readiness [4].

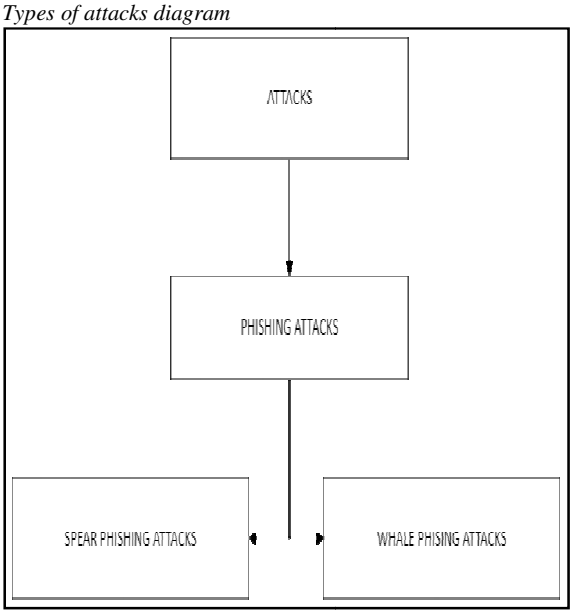
According to Cameron Kent, Maureen Tanner, Salah Kabanda how intrusion detection is perceived and used by SMEs to detect security breaches or unauthorized access or performance reduction of a system or network [5]. According to Brenton Borgman, Sameera Mubarak KimKwang Raymond Choo, The ISMS is implemented to provide an environment that is aware, predictable, sound and appropriately protected and secured from threats and risks to its information management assets. and risks to its information management assets [6].

According to Ms. Sophiya Shikalgar, Ms. Sophiya Shikalgar Ms. Sophiya Shikalgar It is found that phishing attacks is very crucial, and it is important to get a mechanism to detect it and respond early. Machine learning algorithm was used with a classifier to detect and identify and phishing attack, which can be complex. Automated solutions have by used Machine learning [7].

According to Hasika Pamunuwa, Duminda Wijesekera , and Csilla Farkas Phishing is becoming a popular form of fraud on the Internet resulting in disclosure of personal data. Reacting to these attacks, the Internet community has responded by allowing the browsers to setup many methods to detect and warn of potential phishing attacks. Although successful, these solutions [8]. We propose an institution-wide, two-staged IDS system to detect phishing. Our solution performs an initial estimation of phishing email, followed by automated web crawlers visiting those potential phishing sites. Recursive crawling of potentially phishing sites increases the accuracy of the detection whether a web site impersonates another

II. TYPES OF ATTACKS

Figure 1:
Types of attacks diagram



Phishing attack is a type of social engineering when a hacker sends a message to trick the victim to hand over or reveal sensitive information to hackers or to install viruses, ransomware or trojan and hacking for WIFI passwords.

Spear Phishing Attacks

Is a personalized and a more targeted from phishing. The Target is on specific individual's hackers know well about the victims. The email that is generated seems to come from legitimate and trustworthy sources. The email is carefully designed and very professional and tailored for recipient.

Whale phishing Attacks

This are more targeted than spear phishing and targets a senior executives example CEO/CFO.
The emails are crafted with a solid understanding of business language and tone.

IV.DATASETSTRUCTURE ANDDESCRIPTION

In this section, the details of the data set being used for the research are described. Taken from www.Pishtank.com and the name of the dataset phishing. The data set consists of URLs which are labelled as follows non phishing URLs"0" and phishing URLs are "1".

V.METHODOLOGY

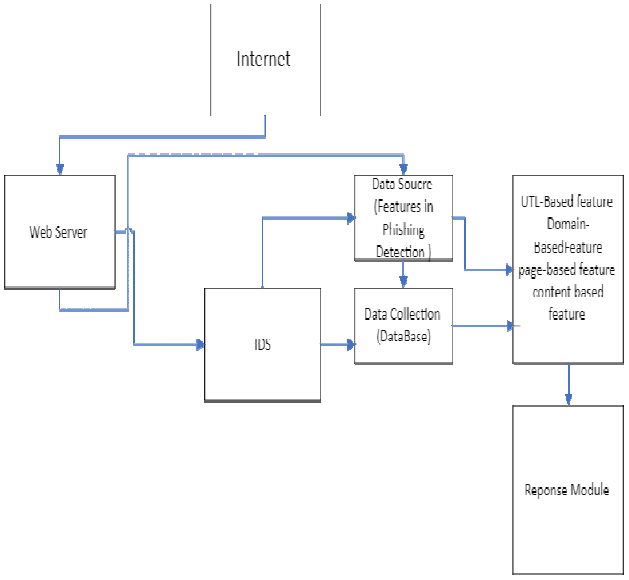
In this section we shall learn about the various classifiers used in machine learning to predict phishing. The proposed methodology to detect phishing websites Classifiers and different methods will be used to check for phishing if its legitimate or not. Machine learning has been widely used in many areas to create automated solutions. By using Decision Tree algorithm to Train intrusion detection system (IDS) to respond to attacks and alert security administrators and create a database of all attacks traced based on the signature. Phishing attacks can be carried out in different ways such as email, websites, malware, and even Ransomware. Input the URL then the next step is feature extraction then classification then determine if it's a phishing site or it's a legitimate site. In this work, we concentrate on detecting website phishing (URL), which is achieved by an Algorithm approach by using different classifiers which will give a good prediction rate and improves the accuracy of the system.

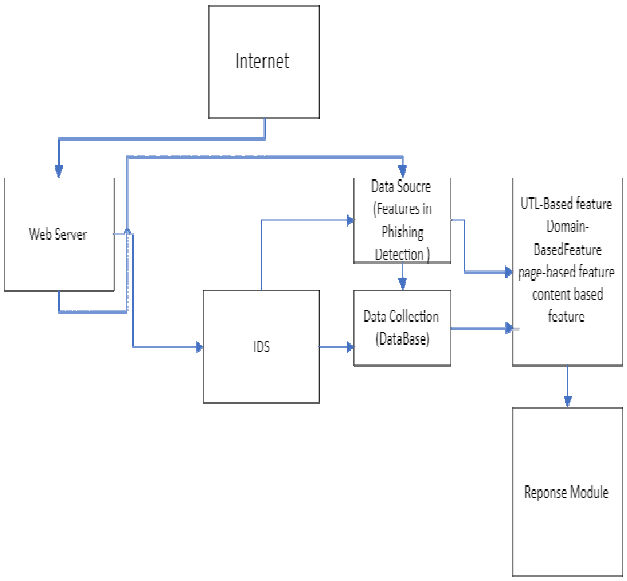
VI.PROPOSED SYSTEM

The proposed system is to detect cyber related attacks using IDS which will help security Administrator to respond and be Ready for future attacks. When developing a model for making predictions, it is necessary to select a specific machine learning algorithm. IDS scans everything that happens in the network including Mail messages and points out some of them as potential phish and enters them into a database. To determine whether it is a phishing attack or not, decision tree was idea and chosen for this research.

The structure of the model can be explained using the flowchart presented in **figure3** first step is to collect the data from and then data is preprocessed then data will be loaded into the IDS to determine the type of threats.

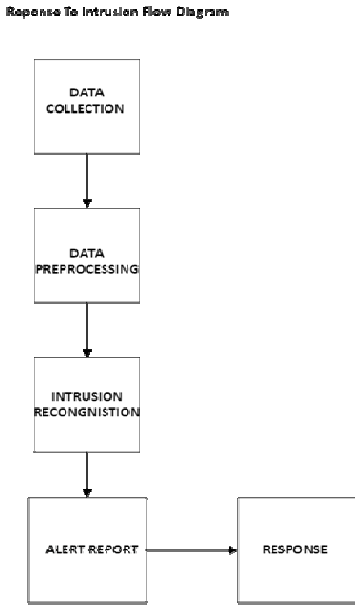
Figure2
Overall Architecture





- The first component is the web server that will send out traffic that will reach the IDS for filtering process, which will detect the type of attack in this case phishing attacks it is an actual or legitimate based on the URL Uniform Resource Locator(URL).The IDS will capture the data based on the types of attacks that have been detected it will respond accordingly.

Figure 3
Flow Diagram



- **Data collection**: It involves collecting network traffic using a software and that help to get the required data.
- **Feature Selection**: The collected data is in large amount due to the network traffic.
- **Analysis:** - The collected data is analyzed in this step to determine whether data is anomalous or not. Here we use various methods for detecting intrusions.
- **Action**: IDS will notify the Security administrator that attack has happened, and it informs him about the nature of the attack. IDS also must participate in controlling the attacks by closing the network port or killing the processes or blocking that phishing attack.
  When assessing the readiness of a critical infrastructure facility, just knowing what to look for is only half the problem. We must do more than just create a large checklist.
  We used Weka, an open-source data mining software, to build a classification model. Weka is a collection of machine learning algorithms for data mining tasks It contains tools for data preparation, classification, regression, clustering, and association rule mining. Figure 2 shows the architecture of the methodology used. After we input the data in Weka, we performed data pre-processing that included setting the appropriate data type and the class attribute. The attributes we selected from the data are the following: 1) awareness of private browsing; 3) awareness of phishing attack; 4) awareness of internet accessibility. We then executed the (decision Model Trees, random forest) classification algorithm and set the classifier rules. We experimented with the training data by splitting the data by 66% into the training data and testing the data.

III. ALGORITHM DESCRIPTION

One of the most widely used algorithm in machine learning is decision tree is a technique in data exploration classification methods for learning models from data and the use of these models for classification. Decision tree are structures used to classify data and with and common and attributes Each decision tree represents a rule, which categorizes data according to these attributes Where each node denotes a test on an attribute, each branch represents an outcome of the test and each leaf node or terminal node hold a class label. The topmost

node in a tree is the root node. Technology. Decision tree algorithm is easy to understand and, easy to implement. Decision tree begins its work by choosing best splitter from the available attributes for classification which is considered as a root of the tree. Algorithm will continue to build a tree until it finds the leaf node.

Decision tree will create a training model which will be used to predict target value or class in tree representation each internal node of the tree belongs to attribute and each leaf node of the tree belongs to class label. In decision tree algorithm, and information gain methods are used to calculate these nodes.

Algorithm for IDS

1. Gathering of data coming from network traffic and
monitoring application log.
2. Feature extraction & Data selection- Select the required data for security analysis.
3. Differentiate between known and unknown packets
Partition the set into subsets using the different attribute
4. Data comparison- Matching selected traffic against
stored rules
5.Detemine if it's phishing attack
6.Store attack in the signature in the data
7. Build a decision tree node containing that attribute
8. Analysis of reports for anomaly detection
Create Legitimate Index

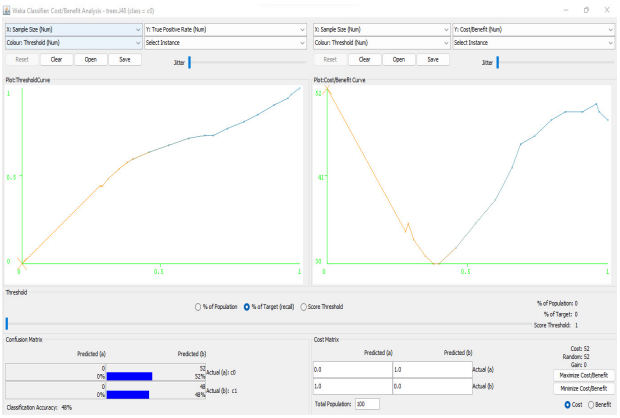
An intrusion detection system observes the activity in a system and chooses whether these activities are malicious or not. Network-based IDS analysis for all activities in network traffic and set up an alarm whenever abnormal activity is observed.

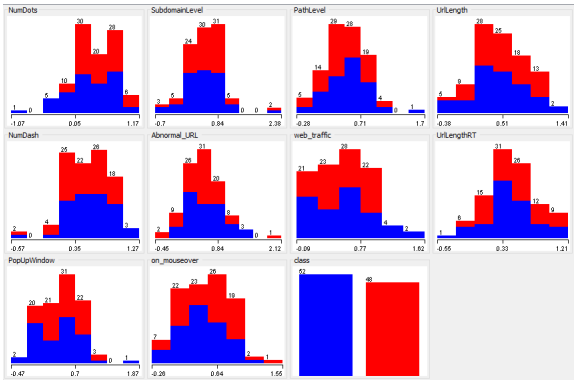
IV. RESULTS AND ACCURACY

WEKA TOOL HAS BEEN USED TO IMPORT MACHINE LEARNING ALGORITHMS. THE DATA SET IS PUT IN TRAINING SET AND THE CLASSIFIER IS TRAINED USING THE TRAINING SET WHICH IS USED TO EVALUATE THE PERFORMANCE OF THE CLASSIFIER.

FIGURE 4

RESULTS OF TEST





The phishing dataset is loaded into WEKA which then generated. Bule is no and red is yes based on the dataset

Table 1

TP Rate	FP Rate	Accuracy	Recall	F-Measure	ROC Area
0.5	0.143	0.833	0.5	0.625	0.679
0.857	0.5	0.545	0.857	0.667	0.679
0.647	0.29	0.715	0.647	0.642	0.679

The shows Decision Tree give a better Accuracy with 0.725. Results will show detection when the percentage of split is 66%.

V. CONCLUSIONS

This research paper is based on how machine learning can be used to improve cybersecurity resilience and readiness. The effectiveness of

cyber security readiness in responding to cyber-attack detection threats. Phishing is a popular form of attack that affects many organizations and leads to internet fraud that involves the disclosure of sensitive information. The proposed system uses Intrusion Detection system (IDS) to detect phishing attacks with high accuracy. IDS can be configured to monitor network packets based on signature and anomaly detections. Decision tree Algorithm is used for the training model which is used to predict the target value or class in the tree representation. Each node of the tree belongs to the attribute and each node (left or right) of the tree belongs to class. Decision tree is a structure that will classify the data and with common attributes [30]. The information gained in by using these methods to calculate the nodes in WEKA using

ACKNOWLEDGMENT

The publication of this work owes to the unwavering support of Dr T. Samraj Lawrence, my supervisor and Dr. Glorindal Selvam, the postgraduate coordinator at DMI ST JOHN THE BAPTIST University, Malawi. Irrespective of their busy schedules, they provided guidance whenever I reached out.

.REFERENCES

[1] Cyber Emergency Response Team for Bangladesh Zakir Hossain, Golam Kibria Zaman and Kazi Abu Taher (Year 2021)

[2] Leeuw KD, Bergstra JA. The history of information security: A comprehensive handbook. Amsterdam (The Netherlands):Elsevier;(year 2007).Anderson JM. Why we need a new definition of information S0167-4048(03)00407-3

[3] Analyzing Security Threats as Reported by the United States Computer Emergency Readiness Team (US-CERT) Yolanda S. Baker, Rajeev Agrawal (year 2013)

[4] Evaluating the cyber security readiness of organizations and its influence on performance. ShaikhaHasanaMazenAliaSherahKurniabRamayahThuras amyc doi.org/10.1016/j.jisa.2020.102726(2021)

[5] How South African SMEs address cyber security: the case of web server logs and intrusion detection (2016) Cameron Kent

[6] Cyber Security Readiness in the South Australian Government Brenton Borgman a,b, Sameera Mubarak a

[7] Kim-KwangRaymond Choo DOI: 10.1016/j.csi.2014.06.002]2nd Edn., Morgan Kaufmann Publishers, Elsevier Inc., USA., ISBN: 10: 1558609016, pp:800.

[8] Intrusion Preventing System using Intrusion Detection System Decision Tree Data Mining 1 Syurahbil, 1Noraziah Ahmad,

[9] American J. of Engineering and Applied Sciences 2 (4): 721-725, 2009 ISSN 1941-7020 © 2009 Science Publications

[10] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," Gaithersburg, MD, Rep. NIST Special Publication 800-94,Feb. 2007.

[11] Shekokar, N. M., Shah, C., Mahajan, M., & Rachh, S. (2015). An ideal approach for detection and prevention of phishing attacks. Procedia Computer Science, 49, 82-91.

[12] Deep Learning Algorithms for Cybersecurity Applications: A Technological and Status Review Priyanka Dixit ∗ , Sanjay Silakari Department of Computer Science & Engg, University Institute of Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya Bhopal (M.P), India

[13]]Review on Intelligent Algorithms for Cyber Security P. Subashini https://orcid.org/0000-0002-8603-6826 Avinshilingam Institute for Home Science and Higher Education for Women, India DOI: 10.4018/978-1-5225-9611-0.ch001

[14] Machine Learning for Cyber Threat Detection Pournima More1Mr.Pragnyaban Mishra/doi.org/10.30534/ijatcse/2020/0891.12020

A Cyber-Security Culture Framework for Assessing Organization Readiness Anna Georgiadou , Spiros Mouzakitis , Kanaris Bounas & Dimitrios Askounis 10.1080/08874417.2020.1845583

[15]]A. Patcha and JM. Park. "An overview of anomaly detection techniques: Existing solutions and latest technological trends".Computer networks. 2007 Aug 22;51(12):3448-70.

[16] Intrusion Preventing System using Intrusion Detection System Decision Tree Data Mining 1 Syurahbil, 1Noraziah Ahmad, 1M. Fadly Zolkipli and 2Ahmed N. Abdalla.

[17] USE OF FIREWALL AND IDS TO DETECT AND PREVENT NETWORK ATTACKS Dr. Abid Hussain

[18] Phishing Website Detection using Machine Learning Algorithms Rishikesh Mahajan.

[19] Datasets for Phishing Websites Detection Grega Vrbanciˇ cˇ a , Iztok Fister Jr.a , Vili Podgoreleca Datasets for Phishing Websites Detection Grega Vrbanciˇ cˇ a , Iztok Fister Jr.a , Vili Podgoreleca(2020).

[20] A review on the readiness level and cyber-security challenges in Industry 4.0, Nikos Benias,Angelos P. Markopoulos(2017)

[21] Intrusion Preventing System using Intrusion Detection System Decision Tree Data Mining 1 Syurahbil, 1Noraziah Ahmad, 1M. Fadly Zolkipli and 2Ahmed N. Abdalla(2009)

[22] A comprehensive review study of cyber-attacks and cyber security;Emerging trends and recent developmentsn YuchongLia,b,

 ©IJSRED: All Rights are Reserved

 ©IJSRED: All Rights are Reserved