iJRASET
International Journal For Research in
Applied Science and Engineering Technology

Volume: 9 Issue: VIII Month of publication: August 2021

DOI: https://doi.org/10.22214/ijraset.2021.37685

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VIII Aug 2021- Available at www.ijraset.com

Network Software Vulnerability Identifier using J48 decision tree algorithm

Shankar Murthy J[1], H L Shilpa[2]
[1]PG Student, [2]Assistant Professor, Department of MCA, PES College of Engineering, Mandya

Abstract: Software vulnerabilities are the primary causes of different security issues in the modern era. When vulnerability is exploited by malicious assaults, it substantially jeopardizes the system's security and may potentially result in catastrophic losses. As a result, automatic classification methods are useful for successfully managing software vulnerabilities, improving system security performance, and lowering the chance of the system being attacked and destroyed. In the software industry and in the field of cyber security, the ever-increasing number of publicly reported security flaws has become a major source of concern. Because software security flaws play such a significant part in cyber security attacks, relevant security experts are conducting an increasing number of vulnerability classification studies, this project can predict the software vulnerability means the software's in the device are authorized or not and who scan the system multiple times, to identify the vulnerability j48 decision tree algorithm was used.

Keywords: Malicious assaults, catastrophic losses, Security flaws, Cyber security, Vulnerability Classifications.

I. INTRODUCTION

The application of the Internet and computers has two effects on industries, thanks to the rapid growth of information technology. They provide convenience, but they also pose significant risks and hidden threats. Information security challenges have recently become more relevant as the level of digitalization in numerous businesses has improved. Vulnerabilities are software and hardware flaws in a system that can be illegally exploited by unauthorized personnel. Once a malevolent attack exploits vulnerability in an information system, the security of the system is jeopardized, with potentially catastrophic repercussions. It is not only possible to enhance the efficiency of vulnerability recovery and management, but it is also possible to lower the danger of the system being attacked and harmed if the vulnerability can be classified and handled efficiently. This is extremely critical for the system's security performance, In the IT industry; we need to develop an effective model for generating software that executes software scans for vulnerability assessments in network equipment.

The architecture of the Attack Simulator and the techniques for generating harmful actions against computer networks are described in this paper. The proposed approach is based on stochastic grammar-based attack models and is implemented through automated imitation of remote computer network attacks of various complexity levels [1].

The network vulnerability assessment to detect malicious behavior and prevent the machine from being exploited by unauthorized third-party software installed on the network-connected computer, as well as the audit of conformities and non-conformities to generate a report. The rapid advancement of computer network systems provides users with both significant convenience and new security threats [5]. Vulnerability assessment is the process of discovering, quantifying, and emphasizing (or rating) the vulnerabilities in a system in this proposed system. A vulnerability assessment is carried out to identify the weaknesses in information systems that could be exploited, resulting in a data breach. The vulnerability assessment models in the application breakthrough are capable of understanding risks and defining a response for them. The proposed approach proposes an application that includes an automatic notified and a scan validator.

II. LITERATURE SURVEY

The software tool "ATTACK SIMULATOR" is used to evaluate network security rules throughout the deployment and design phases of systems. It describes the simulator architecture and generates malicious attacks in real-world networks. Well, there are numerous causes for the security complexity assurance, including the number of users, the number of threats targets within the system network, and so on. The purpose of this study is to use a software tool to analyses computer network vulnerabilities using MASDK (Multi Agent System Development Kit) [1].

In paper [3] focuses on computer network security vulnerabilities. They argue that before we can solve the problem that develops in the computer network, we must first discover the reasons of the vulnerabilities. Hackers can't access the actual one using sophisticated scans and encryption techniques; therefore access verification prevents the vulnerability. Some of the problems (1)

Subsistent technique for vulnerability (2) Open question of the Subsistent detection technique namely (a) Encrypt method (b) Notice (c) Advance of new defense measure, etc. In [5] sounds into the known vulnerabilities in computer networks. They argue that before we tackle the problem that develops in the computer network, we should first discover the reasons of the vulnerabilities. Hackers can't access the real one using sophisticated scanning and encryption techniques, therefore access verification prevents the vulnerability.

Here, they uses Real-time LAN acquisition data, traffic capturing using wire shark program, and the algorithm they include is RC2,RC4,DES,3DES then the accuracy between 65-83%.Vulnerability in software Faced with so many obstacles, an attacker delivers a malicious virus via phishing to destroy the host machine and steal the contents of the database information stored. As a result, the system administrator must put the effort first, and cyber security professionals must keep a watch on the system at all times. Technologies they used Nmap tool, Using Nessus, Openvas [6].Metric based comparison is done to obtain the degree of vulnerability assessment and based on the weight the software analysis based on the situation and identify the defect proneness.Metrics:(1)NumofLn(2)NumofFn(3)AveCCofFn(4)IntofLn(5)IntofOut(6)ClusCoeofNod. They used these algorithms: MFSA, BN, NB, NN, SVM, RF .Accuracy is about 80-91%.[8]

[9] Madae Zolanvri, includes Machine Learning to analyses the network vulnerability of IIOT (Industrial Internet Of Things) IIOT it refers to the Interconnected sensors, Instrument's and other devices networked together with computers industrial applications. Here they deploy backdoor, command injection and SQL .Main purpose of using IIOT in this paper is taking a huge advantage of IOT in the Industrial Control System's(ICs) they looking for Protocols ex: Madbus,DNP3,BACnet, and more. In [2], Sheraz discussed IEEE 802.16e. DOS [Denial Of Services] attacks in this particular vulnerabilities this includes unprotected entry, unencrypted communication, Managing frames and weak key for the mechanism in Multi and broadcast operation .Here, they are looking for Dos attacks on IEEE 802.16e Security, Multi and broadcast services shared keys vulnerability, WiMAX as well they used a technique Cryptographic keys.Also, The Authentication Mechanism of the IEEE 802.16e it should be extended, we are going to the last step of this IEEE 802.16e. it is actually a Robust and very promising Security vulnerability architecture. We Come to know about above thesis papers they are going to explain the vulnerabilities in a different ways like technologies they used to find out the vulnerabilities, some of them uses deep learning technologies, SVM algorithm, RC2, 3DES more.

III.PROPOSED SYSTEM

[5] Vulnerability assessment is the process of discovering, quantifying, and prioritising (or rating) the vulnerabilities in a system in this proposed system. A vulnerability assessment is carried out to identify the flaws in information systems that could be exploited, resulting in a data breach. The vulnerability assessment models in the application breakthrough are capable of understanding risks and defining solutions for them. Using Visual Studio 2015, the suggested model proposes an scan checker application. Here is an advantage using this proposed system NSVI (Network Software Vulnerability Identifier) i.e. Automated Scanner makes easy to scan system without manual effort, Log mapper and notifier makes work faster and efficiently, less expensive compare to presently using in big companies, trustworthy and effective in mid and large sized companies due to scalability.

A. Methodology

In Fig-1 Admin will add software's to the system time to time as the company regulates, with respective software id as well as the details. The user IDs and passwords will be generated programmatically, and those IDs and passwords will be sent to the admin, the application scans the system software's. before that user have to register after login to the application , The user register to the application then admin come into picture admin verify the user and accept credentials what the user gave. Then user login to application and scan the system software's and perform audit to view unauthorized software's lists, admin add or delete the software's by time to time as the company regulates, and admin focusing an eye to the audit log reports then verify that reports . Using the j48 decision tree algorithm we can predict the software's are authorized or not, the accuracy of algorithm works in this project about 75-85%.

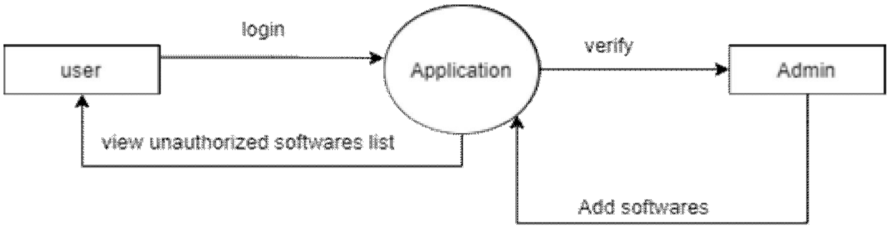

Fig-1: System architecture

B. J48 (Decision tree) Algorithm

Fig-2 represents decision trees are a kind of Supervised Machine Learning (SML) during which data is continually separated supported a parameter. Two entities, decision nodes and leaves, are often wont to explain the tree. The selections or final outcomes are represented by the leaves and also the data is separated at the choice nodes. The Decision Tree algorithm is a component of the supervised learning algorithms family. The choice tree approaches, unlike other supervised learning algorithms, are often utilized to unravel regression and classification issues.

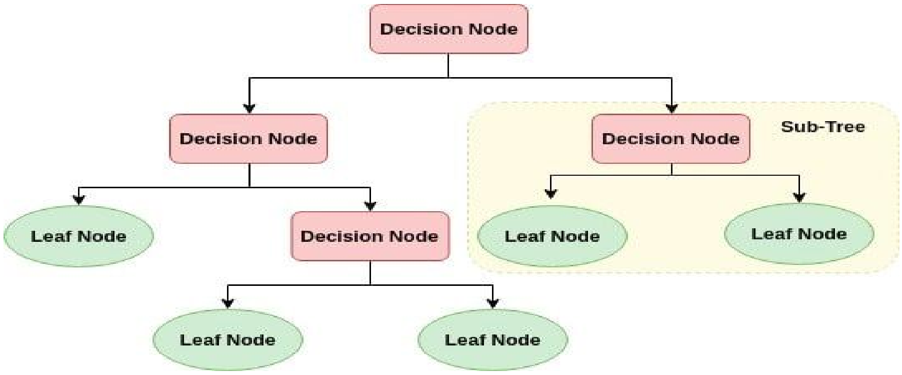

Fig-2: J48 (Decision Tree) Algorithm

C. Construction of Decision tree

Through the use of a characteristic fee test, it's possible for you to to "learn" the tree. On each subset derived from it, recursive partitioning is applied. In other words, it's finished when all nodes' subsets have equal fees, or when splitting no longer provides fees for the predictions. In addition, the choice tree classifier can be created with no prior knowledge of a particular area or parameter settings, making it ideal for exploratory expert knowledge discovery. Decision timber is able to handle a large amount of dimension data. The choice tree classifier, which is currently in vogue, is extremely accurate.

By sorting instances down the tree from the root to a leaf node, decision trees can classify instances. When an instance is classified in this way, it is done by starting at a root node and looking at its attributes, then moving up the tree according to its attribute value. The subtree rooted at the new node is then processed in the same way as the original subtree.

D. Decision tree Representation

Instances are classified using decision trees by sorting them down the tree from the root to a leaf node, which provides the classification. As indicated in the above diagram, an instance is classified by starting at the root node of the tree, checking the attribute specified by this node, and then progressing along the tree branch according to the attribute value. The sub tree rooted at the new node is then processed in the same way.

1) *Step1:* Place the best attribute of the dataset at the root of the tree. To that we have calculate **Entropy**Entropy, also called as Shannon Entropy is denoted by H(S) for a finite set S, is the measure of the amount of uncertainty or randomness in data.
2) *Step2:* Subdivide the training set into sections. Subsets should be created so that each subset has data with the same attribute value. Make that attribute a decision node, then use the learned dataset to split the dataset into smaller subgroups. The next step is to select the attribute that will provide us with the most information gain.
3) *Step3:* Predict the incursion type using the classified values from the preceding algorithm. Repeat on each step subset until you've found leaf nodes .

E. Psuedocode

```
1) Input: Read the system
2) Output: Unauthorized list
a) Start
b) Define counter is Zero
c) For  i is less than ListBox1.Items.Count
d) Increment i
e) For j is less than snames.Count
```

f) Increment j
g) If counter is not equals to 999
h) Open if
i) Unauthorized software's
j) End if
k) Stop all

F. Log Statistics

In fig 3 indicates statistics of the user he scans the system and how many times he perform the audit and user approve all things are shown in the figure user fully perform the audit to scan the system and trying to fetch the reports are generated by the software automatically , that softwares list copy was sent to the admin as well after that admin come in to picture he identify the user whether he is a person not harm to their company details or this person is good he is not doing such things . these are all control under the admin he confirm the user to perform audit if he didn't confirm then user cant fetch the reports.

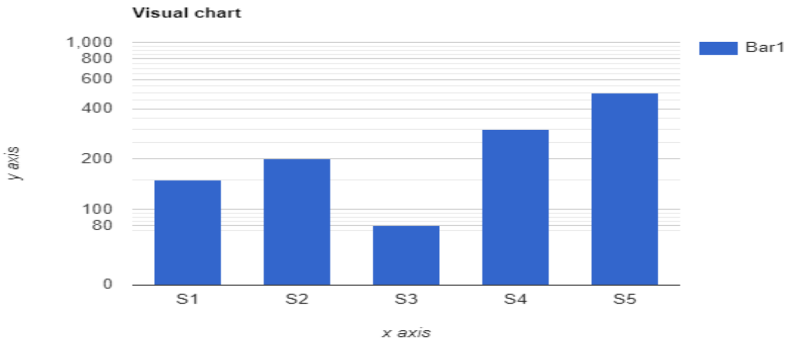

Fig-3: Log Statistics

IV. CONCLUSIONS

A vulnerability scanner developed in this project is an application that is used to scan the software and provide a report when the vulnerability is detected. It is a web based application which deals with crucial aspects of security i.e. Scanning for Network Vulnerabilities The data gathered from the network. It compiles a vulnerability list from Network Devices.

In future this work can be extend to identify vulnerabilities in Next Generation firewall, Web application Firewall, Intrusion detection system, Web and Email Gateways, which helps in every circumstances either in companies or personal purpose .

REFERENCES

[1] Kotenko, Igor. "Active vulnerability assessment of computer networks by simulation of complex remote attacks." 2003 International Conference on Computer Networks and Mobile Computing, 2003. ICCNMC 2003.IEEE, 2003.

[2] Nasser, Sheraz, Muhammad Younus, and Attiq Ahmed. "Vulnerabilities exposing IEEE 802.16 e networks to DoS attacks: A survey." 2008 Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing. IEEE, 2008.

[3] Fu, Cuijiao. "Research of Security Vulnerability in the Computer Network." 2010 International Conference on Biomedical Engineering and Computer Science. IEEE, 2010.

[4] Sun, Shiguo, et al. "The Research on Network Vulnerability Analysis Methods." 2012 Second International Conference on Intelligent System Design and Engineering Application. IEEE, 2012.

[5] Yan, Fan, Yang Jian-Wen, and Cheng Lin. "Computer network security and technology research." 2015 Seventh International Conference on Measuring Technology and Mechatronics Automation. IEEE, 2015.

[6] Wang, Yien, and Jianhua Yang. "Ethical hacking and network defense: choose your best network vulnerability scanning tool." 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA). IEEE, 2017

[7] Mostovich, Daria, et al. "High-level vulnerabilities of software-defined networking in the context of telecommunication network evolution." 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus). IEEE, 2017.

[8] Wei, Shengjun, et al. "Vulnerability Prediction Based on Weighted Software Network for Secure Software Building." 2018 IEEE Global Communications Conference (GLOBECOM). IEEE, 2018.

[9] Zolanvari, Maede, et al. "Machine learning-based network vulnerability analysis of industrial Internet of Things." IEEE Internet of Things Journal 6.4 (2019): 6822-6834.