INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A UNIFIED APPROACH FOR MEASURING AND CLASSIFYING THE RISK OF UNKNOWN VULNERABILITIES

J. Jeyaseeli[1], Dr. D.C. Joy Winnie Wise[2], B. Priya[3]

[1]PG Scholar, Dept of CSE, Francis Xavier Engineering College, Tirunelveli, TamilNadu, India.
[2]Professor & Head, Dept of CSE, Francis Xavier Engineering College, Tirunelveli, TamilNadu, India.
[3]Asst Professor, Dept of CSE, Francis Xavier Engineering College, Tirunelveli, TamilNadu, India.
graciejeya@gmail.com, joywinniewise@yahoo.com, Ph: +91 7373636633

Abstract: - The main objective of this project is to find the vulnerabilities caused due to zero day attack. Through vulnerabilities present in the systems that are in the network, the attackers can reduce the certainty of the system. In previous papers they used zero day safety to identify the vulnerabilities. But it is more complex to implement. To avoid the complexity to identify the vulnerabilities we use K-Zero day safety to find the vulnerabilities. Initially in this project we use K-Zero day safety to take the count of the zero day vulnerabilities present in the network which is taken into account, and then we use the ELM classification to classify the type of vulnerabilities. By this we can find the type of vulnerability that causes the risk of the particular network. The ELM is a good to be used for classification.

Keywords*:* Network, Vulnerabilities, Zero day attack.

1. Introduction

A computer network is similar to a neural network. It is not just some connection, a network comprises of various components that are connected either by wired or wireless links. The basic operation of a network is to transfer data from a source to destination through one or many hosts. The host may include all the devices in the network like computers, routers, firewalls etc., and host is also called as nodes. The host performs originating, forwarding and terminating of data. The data is sent in packet from source to destination. Since various devices are present in the network for transferring the data it is liable to weakness like vulnerability through which the attacker can access data from the network without authentication i.e. there is possibility of unauthorised user accessing the data. This may lead to the breach of network security.

When an attacker or hacker wants to access data from the network initially they check for the possible weakness or vulnerability in the network. The vulnerability in the network makes the network error prone and failure in the data transfer. This causes the lack of network security which leads to various problems like loss of data, data corruption. Since the entire human race depends on the data or the information present in the computer networks it is very important to secure the network. And there are hackers who are in need of the data available in the network were they actively involved in the process of obtaining the data from the network. It is essential to be aware of the attackers present in the network which is taken into consideration.

Considering the weaknesses in the network, most of them are discovered by the fundamental security mechanisms or by using firewall but when a hacker wants to access they try to abuse the network by discovering

the errors that are unknown or unidentified firewall or other security mechanisms. One such error or weakness in the network is a zero day attack. Zero day error can be found among the devices that are present in the network. The attacker instead of hacking the links they try to use the zero day error present in any one of the devices in the network which act as host in forwarding or receiving the data. Zero day error is a minor error generated in the devices during the development process of the devices by the vendor which they had zero days to spot them.

2. Methodology

A. Nodes Information:

To instantiate the network model we need to collect information about, Hosts (e.g., computers, routers, switches, firewalls, etc.), Connectivity between hosts, and for each host, its remotely accessible services, Security mechanisms and services, and privileges. Such information is typically already available to administrators in the form of a network map or configuration database. A network scanning will assist in collecting or verifying information about hosts, connectivity, and services. Nonetheless, a close examination of host configurations (including firewall rules) is still necessary because network maps and network scanning will usually not reveal hidden or disabled services or connectivity (which may be re-enabled through zero-day attacks and, thus, must be correctly modelled), and privileges are often best identified by examining the host configuration. Collecting and maintaining such information for a large network certainly involves substantial time and efforts. However, we note that a key advantage of our model is its exclusion of local applications and services (modelling which would be infeasible for most networks). Focusing on remote services allows our model to stay manageable and scalable, considering the fact that most hosts typically only have a few open ports, Initialize theses nodes, to collect the information of the nodes. This node information is given to the K-Zero Day safety to count the vulnerabilities.

B. K-Zero Day Safety:

In this module of the project, the safety algorithm to find the zero day attacks is used. The main principle of this safety algorithm is to look for the services, connectivity and the privileges rather than looking for the underlying details. Initially we consider the entire host including all the devices in the network that are prone to zero day attacks which includes firewalls too. Then we include the presently inactive devices. Finally the services those are present far apart. The main idea of this project is that we cannot assume the specific property of vulnerability; instead it depends upon the property of the vulnerabilities that are grouped together. We may not know about the zero day attack but we known that zero days needs a network connection to take advantage over the network using the source and the destination. By taking advantage over such weakness leads to a special benefit over the destination host.

C. Classification:

After collecting the information about the nodes (hosts) present in the network and applying the safety algorithm it's time to classify. To classify the attacks due to zero day weakness ELM classification is used. In elm using the collected information, every nodes in the network is traversed using two different course; chief course and peripheral course. The chief course identifies the behavioural change logical processing and persuasion. Whereas peripheral course involves low effort compared to the chief course as it involves with the external devices

3. Related Works

In [1] Hannes Holm, Mathias Ekstedt and Dennis Anderson, says that security modelling with Common Vulnerability Scoring System does not describe the detailed and correct data about the time to compromise of a system single handed. And the result shows that modelling with Common Vulnerability Scoring System is more closely connected with the time to compromise. As a result the model that uses weakest link to combine a metric is less successful than those consider all vulnerabilities.

In [2] Muhammed Shahzad, Muhammad Zubir Shafiq and Alex X, done examining measurement including seven aspects they are, phase in the lifecycle of vulnerability; evolution of vulnerabilities; functionality of vulnerability; the right to gain advantages of the available weaknesses; vulnerabilities level of risk; software designer; software products. Their examining process revealed many possible effects for software development and deployment.

In [3] Nwokedi Idika and Bharat Bhargava, propose a well expressed graph based security metrics and an algorithm for interconnecting the usage of those metrics. They presented a prototypic result that gives a final conclusion.

In [4] Ratinder Kaur and Maninder Singh, proposed a detailed survey to give the abstract of the efforts related in finding the modern zero day threats in form of the zero day polymorphic worms, which the traditional security and defences missed to find.

In [5] Zhinchun Li, Manam Sanghi, Yan chen, Ming-Yang Kao and Brain Chavez proposed a network based signature generation system that take place automatically for polymorphic worms, which is a wise model to examine the invariant nature of the worms from different stages, that allows to make logically quick attack generation algorithm.

4. System Design

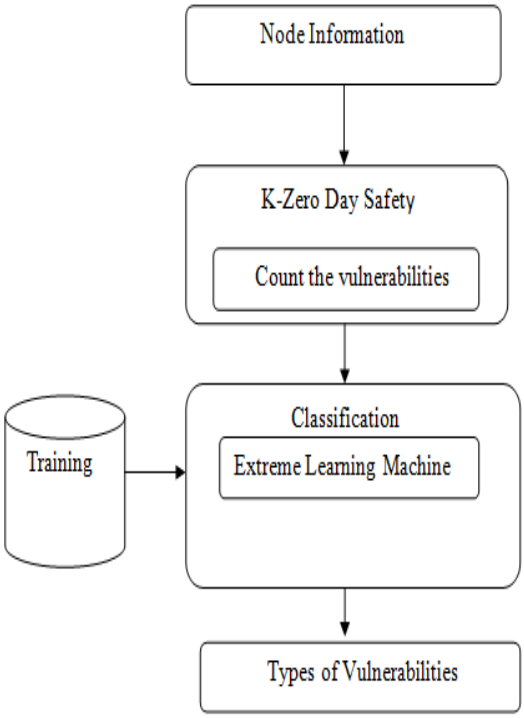

Figure 1: System Architecture

5. Conclusion

This project proposes the K-Zero Day Safety to count vulnerabilities. Once the node is initialized, the node information is collected. Then apply the safety algorithm. This is applied to separate out the vulnerabilities. To classify the type of the vulnerabilities ELM algorithm is used. It is considered to be one of the best techniques used for classification. Thus the proposed system shows a good performance.

Acknowledgment

I convey my sincere thanks to Dr. D. C. Joy Winnie Wise Professor and Head, Department of Computer Science and Engineering, Francis Xavier Engineering College who inspired me and guided me throughout and it is a privilege to express my gratitude to her.

REFERENCES

[1] Hannes Holm., Mathias Ekstedt. and Dennis Anderson. (2012) 'Empirical Analysis of System-Level Vulnerability Metrics through Actual Attacks', IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 6.

[2] Muhammed Shahzad., Muhammad Zubir Shafiq. and Alex X. 'A Large Scale Exploratory Analysis of Software Vulnerability Life Cycles'.

[3] Nwokedi Idika. and Bharat Bhargava. (2012) 'Extending Attack Graph-Based Security Metrics and Aggregating Their Application', IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 1.

[4] Ratinder Kaur. and Maninder Singh. (2014) 'A Survey on Zero-Day Polymorphic Worm Detection Techniques', IEEE Communications Surveys & Tutorials, Vol. 16, No. 3.

[5] Zhinchun Li., Manam Sanghi., Yan chen., Ming-Yang Kao. and Brain Chavez. 'Hamsa: Fast Signature Generation for Zero-day Polymorphic Worms with Provable Attack Resilience', University Evanston, IL 60208, USA.