International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)
ISSN (Online) 2349-6967 *Volume 2 , Issue 1(Jan-Feb 2015), PP1-5*

Quantifying Network Security Level Using Probabilistic Security Metric And Attack Resistance Metric

Swarupa V. Mohite[1]
[1]*(Department of Computer Engineering. Y. Patil College of Engineering and Technology, Kolhapur.)*

Abstract:- Nowadays network security threats are increasing; proportionally multistage and multiple host attack scenarios are also increasing. So these scenarios must be considered while assessing the network vulnerability towards attacks. One of the solutions to network vulnerability problem is to construct an attack graph for network configuration. Attack graph has number of attack paths which are nothing but sequence of exploits. And attacker tries to reach the destination with help of these paths. Each attack path represents an attack scenario. As the number of attack scenarios increase, the overall security of the network reduces. Thus there is need of security level quantification of given network. In this paper, a security approach is provided and two security metrics are used to evaluate the relative security levels of network configurations, those metrics called probabilistic security metric and attack resistance metric. A case study has been presented to demonstrate the applicability of the proposed approach.

Keywords: - HiCuts, Attack Graph, Security Metric, Packet Classification, Security Quantification

I. INTRODUCTION

Networks are large networks and small networks, but size of network is irrelevant in terms of importance of network security. The intent behind network security is to guard the network and its component parts from unauthorized access and mistreatment. Network security system is an important component of the configuration as well as network management. Network security is a technique which protects the basic networking infrastructure from an unlawful access, alteration, damage or wrong usage. This gives a protected platform for computers, programs and various users to execute their permissible vital functions within a secured environment.

Various network security scanners are available which are able to detect vulnerabilities local to a system. But these scanners are not efficient to identify multi-stage and multi-host attacks[1]. In practice, some vulnerability may still stay behind in a network after they are discovered because of environmental factors and cost factors. To eliminate such remaining vulnerabilities there is a need to assess and quantify the possibility that attackers may compromise significant resources through combining different vulnerabilities.

Currently in network security, focus is on qualitative nature of security, rather than quantitative study of network security. For assessing overall security of a network, it require to understand the interplay between host vulnerabilities thoroughly. Such an understanding is difficult to obtain with vulnerability scanners and IDS.

One such tool which gives explanation about the correlated attacks is attack graph[1][3]. An attack graph consists of a number of attack paths each of which shows an attack scenario. Therefore, as more the number of attack paths and attack scenarios, higher is the probability of compromising a target. Thus, there is need for quantification of security level of a given network.

In the proposed system work, behavior of incoming packets and their characteristics are studied, analyzed and used in detection process of suspicious and unidentified packets. All network packets are captured and examined. For identification of packets, packet classification algorithm HiCuts is studied and implemented. Construction of attack graphs are done for showing attack paths with more clear representation. The final result of implemented work is showing detected suspicious unknown packets and safe packets, appropriate actions taken on suspicious packets and total security strength of network. In next section II we are presenting the literature survey over various methods of network configuration. In further section III, the proposed systems' approach and its detail system architecture diagram is depicted. In section IV we are presenting the current state of implementation and results achieved. Finally conclusion and future work is presented in section V.

II. LITERATURE SURVEY

According to Nirnay Ghosh., S. K. Ghosh [1], many network security scanners are available and are only capable of detecting local vulnerabilities. But they cannot identify all conditions which are responsible for complete attack to take place, or how various vulnerabilities existing on different systems may be combined to generate multi-stage, multi-host attacks.

The work has been done by Balzarotti et al [2] where they were using functions for modeling the effect of executed exploits on the resistance value of other exploits. However, their work focuses on computing the minimum effort required for executing each exploit, whereas it needs to compute the overall security of a network with respect to given critical resources.

For assessment of overall security of a network, thorough understanding of the interplay between host vulnerabilities is required. That is, how and which vulnerabilities can be combined for an attack. L. Wang, A. Singhal, and S. Jajodia [3] concluded that the existing tools focus on identification of individual vulnerabilities or attacks, and are usually unaware of the relationships between vulnerabilities or attacks so there is need to detect such correlated attacks.

III. PROPOSED APPROACH

Proposed security system works for training and testing dataset, generation of attack graphs, which will help to detect, correct and prevent existing network from various attacks and analyze the security straight of a network. Figure 1 shows Architecture of proposed security system. It has five steps: identifying individual exploit conditions, identifying relations between exploits of different nodes, representing attack graphs, performing respective preventing, corrective actions for the detected attacks and quantifying the security strength of network.

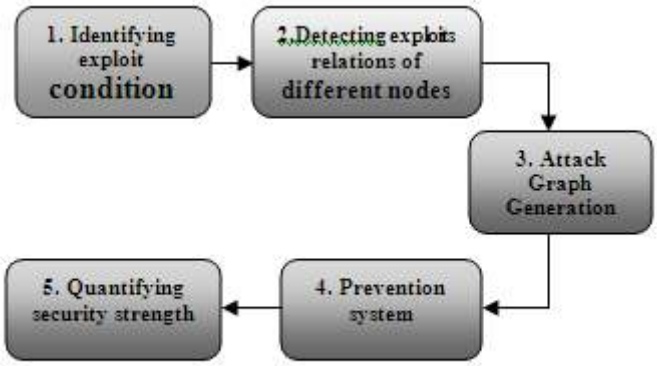

Fig 1.Architecture of proposed security system

This mechanism is present on each host in the network, and will find the exploit conditions having conjunctive and disjunctive relations between vulnerabilities and generate appropriate attack graph. This attack graph will help to show relationship of exploits of various nodes and will help in performing preventive and corrective measures for exploit conditions. Total security level of network configuration is analyzed using various security metrics.

IV. SYSTEM DESIGN

4.1. Identifying exploit condition

For exploit condition identification; packet capturing, training and testing activities are done. Firstly each node in the network is needed to be trained with safe data transactions as training activity. From the training data rules are created. Sample of data rules as follows:

@192.168.1.3/32 192.168.1.1/32 375 : 383 375 : 383 0x06/0xFFFF
@192.168.3.141/32 192.168.3.141/32 0 : 100 0 : 100 0xFF/0xFF

These rules contains source IP address, destination IP address, Packet size at source, Packet size at destination, ports used etc. These saved rules get used in detection process. After that, system build HiCuts decision tree internally with packet classification algorithm. This tree has all the rules stored with it and then onwards it works as a model for testing phase i.e. exploit condition detection mode. Each time a packet arrives in network, previously created decision tree is navigated to find a leaf node. Each leaf node stores a small number of rules. Linear searches among these rules yield the packet parameters matching. Packets with matched rules are known to be safe and hence sent to destination and others are suspicious and hence blocked and represented with red color. Likewise the system is enabled to identify individual exploit conditions on single node.

4.2. Detecting exploit relations of different nodes

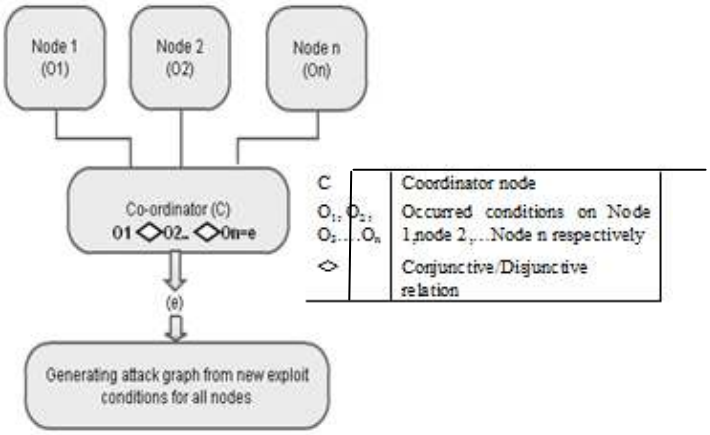

Fig. 2 .Generation of new exploit conditions by combination of existing conditions.

Figure 2 shows the procedure of selecting one node as a coordinator node among all the existing nodes. The role of a coordinator is to discover the combinations of conditions occurred on multiple nodes which will generate some new exploits and are called multi-host attacks.

Every node can send its own list of occurred exploits to attack graph generation module. For detection of combined exploit conditions, coordinator update with all exploits lists of other nodes. So for this reason each node sends its current exploit list to coordinator. The coordinator will check for likely relations between all combinations of exploits and conditions. The relation can be conjunctive or disjunctive relation. The Coordinator synchronizes all exploit lists. And then send new updated exploit data to all the client nodes to improve their advance detection process.

4.3. Attack Graph Generation with attack Prevention and correction process

According to the process of detection of individual and related exploits, particular actions are taken on safe and unidentified packets. All the matched packets are allowed inside the system and suspicious unknown packets are blocked. Blocked packets are represented with red color and safe are shown with white color.With help of this data, complete attack graph is generated. An complete attack graph is actually achieved by connecting all individual nodes' graph. This attack graph will be used to classify the vulnerabilities leading to possible attacks and possible cumulative attacks. It is also used to identify the measures for further attacks [4].
From the attack graph , we can figure out that which nodes are affected by exploits, which are source of the exploits or through which in-between nodes exploit conditions are transmitted to target node.

4.4. Testing network security and performance

The implemented system is tested with different conditions like conjunctive and disjunctive relations between the exploit conditions. Analysis of achieved results elaborates the effect of system on network security and its performance. The mathematically quantification of security strength of a network system is done with help of security metrics: probabilistic security metric and attack resistance metric.

Wang et. al. [3] have proposed a metric called as probabilistic security metric; which quantifies the probability of successfully executing an exploit and measures the likelihood of compromising a network in terms of the fraction of attackers reaching the goal. Therefore, this metric can be used to measure the degree of security strength for a network configuration. For an exploit e and condition c, the probabilistic security metric is given by two scores [6]-

• Individual score- It defines the intrinsic likelihood of execution of an exploit or a security condition, denoted by p(e) and p(c) respectively. This score is assigned based on expert knowledge about the vulnerability.

• Cumulative score- It measures the fraction of attackers who successfully reach an exploit e or a condition c, denoted by P(e) and P(c) respectively. This score is evaluated using the probabilities of independent and non-mutually exclusive events. For an exploit *e* if preconditions *c*1 and *c*2 are required to be satisfied simultaneously, the cumulative score for the exploit e is given by

$$P(e) = P(c1).P(c2).p(e) \quad (1)$$

Similarly, if a post condition c requires either of the exploits e1 and e2 or both to be satisfied, the cumulative score for the condition c will be given by the formula for calculating the probability of occurrence of two non-mutually exclusive events as, $P(c) = p(c).(P(e1) + P(e2) - P(e1).P(e2))$

An attack resistance metric [3] of a network configuration is a composition of measures of individual exploits. The resistance of an exploit is interpreted as the effort that an attacker requires to put in until success i.e. successful execution of the exploit. Reciprocal of probability of success gives the number-of-attempts (effort) required until success is achieved. Two basic operators for computing *attack resistance* of an exploit are as follows:-

$\oplus$ Operator - This operator is used to realize the scenarios where a disjunctive relationship exists between two or more exploits to successfully execute a different exploit. If r1 and r2 are the individual attack resistances of two exploits e1 and e2 respectively then,

$$r1 \oplus r2 = \frac{1}{\frac{1}{r1}+\frac{1}{r2}} \quad (2)$$

$\otimes$ operator - It is used to realize the scenarios where a conjunctive relationship exists between one or more exploits for successful execution of another exploit. If r1 and r2 are the individual attack resistances of two exploits e1 and e2 respectively then,

$$r1 \otimes r2 = r1 + r2 \quad (3)$$

R- Cumulative attack resistance (R) values are calculated using individual attack resistances r which is generated after executing each instantiated exploit. Likewise using these security metrics, P(C) and R values are calculated, which represents final security strength of the current network.

V. IMPLEMENTATION

For system training, all safe system transactions are captured using WinPcap and with that proposed system is trained with the safe data. After training process, duplicates are removed and data normalization is done. Rule creation is done by analyzing packet parameters as ranges of port values used, packets sizes, protocols used, source IP's, destination IP's. Hierarchical Intelligent cuttings packet classification algorithm is used for Packet classification. Hierarchical Intelligent cuttings packet classification algorithm is a multi-dimensional packet classification algorithm[7]. It pre-processes the rules of packet classification to build a decision-tree for field-dependent search, and in each leaf-node of the decision-tree, a small number of rules bounded by a threshold. After training part, system works in detection mode. Every time a new packet arrives in network, already created decision tree is traversed to find a similar leaf node. Linear searches among these rules yield the packet parameters matching. System is trained such that the packets with known and acceptable parameters are only delivered to desired destination and rest packets will be blocked.

For combined exploit conditions detection, coordinator gets updated with new rules i.e. system gets re-trained after every 10 seconds with exploit lists of all other nodes automatically. The coordinator checks for possible relations between all combinations of exploits and conditions and detect is there any new generated exploits present or not. If there are new generated exploit present then this data is sent to all the clients to update and improve their detection process.

The exploit detection process results are sent to Attack graph generation [9]. Generated attack graphs identify all vulnerabilities leading to possible attacks and possible cumulative attacks. And it is also helpful for recognizing measures for further attacks. Finally by calculating security metrics like probabilistic security metric[5] and attack resistance metric; mathematical quantification of security strength of a network is done.

VI. RESULTS OF PRACTICAL WORK

Following explanation and figures show Results of Practical Work

Individual nodes in the network are trained and tested for vulnerabilities and then for detection of combined exploit conditions, coordinator gets update with the exploit lists of all other nodes automatically after every 10 secs. This new generated exploit data is sent and helps all clients to improve their detection process i.e. all clients synchronizing rules with rules of coordinator.

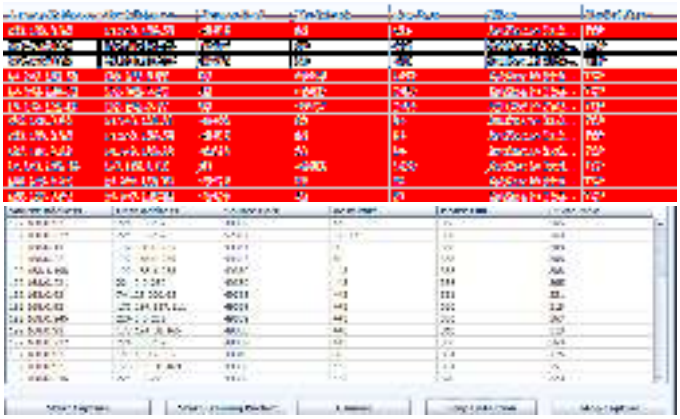

Fig. 3.Detection and Prevention

As shown in Figure 3 system works in detection mode. Every incoming new packet is checked with generated rules of training, by traversing the HiCuts decision tree and only packets with matching rules are known to be safe so delivered to correct destination and shown in white color in window, while others are suspicious so blocked and marked with Red color.

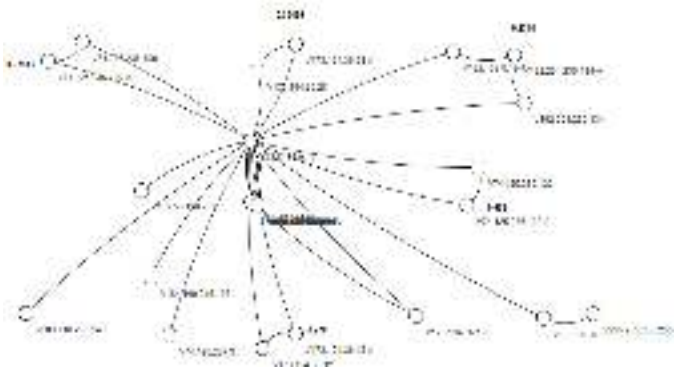

Fig .4. Generated Attack Graph

Figure 4 shows attack graph for current state scenario having both safe and suspicious communication. Here, vertices of attack graph are divided into three categories:-server, clients and all addresses of websites communicated. To demonstrate the safe communication, edge connects vertices indicating client and website address. And to show suspicious communication or attacking condition, edge connects vertices represented with client and website address which is appended with –A .

If any of communication has some safe transactions and some of the attacking transactions then vertices are duplicated and one is showing just the address of communicated website and other appended with –A.

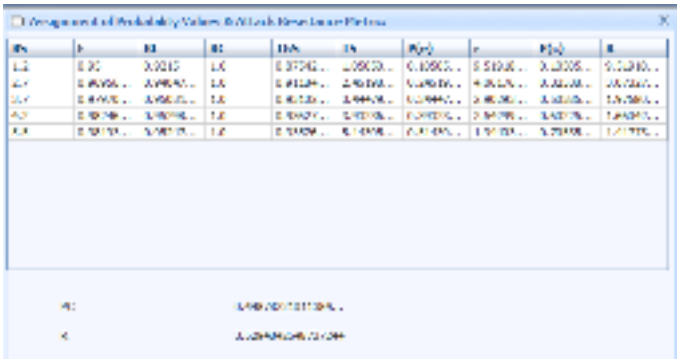

Fig.5.Quantifying the security strength with P(C) and R

Average P(C) and R values are derived by calculating probabilistic security metric and attack resistance metric, as shown in Figure 5. The cumulative probability score P(c) is calculated for all the nodes of the attack graph to determine the fraction of attackers successfully compromising the goal and cumulative resistance (R) for each attack path reaching the goal can be computed by simply adding individual resistance values along the path. So the end values are:

P(C) = 0.448

R = 3.52

Result shows that cumulative resistance of the whole network should be smaller than the cumulative resistance of each possible attack path. If number of attack scenarios is less then it offers more resistance to external attacks.

VI. CONCLUSION AND FUTURE WORK

This system is using the method in which continuous monitoring of new incoming packets is done. Every node in the system is trained and tested for HiCuts. By considering relations between the exploits on different nodes it detects attacks and generates its attack graph. Security quantification is done as we can get the values for probability of successfully executing an exploit and fraction of attackers reaching their goal. So final result of the system is secured network for individual and related attacks.

In future there is a vast room to improve the performance of the system by improving the techniques and algorithm we applied. Like HiCuts packet classification algorithm can be improved for memory usage, classification speed and lower run-time. Attack graphs also have scope to improve because it has disadvantage regarding complexity in visualization. As the number of hosts and vulnerabilities increases, the complexity of attack graphs boosts rapidly, preventing the administrator from understanding the graph and extracting remedies manually. So attack graphs can be replaced with Attack grammar [10]. Our aim is to improve the performance of the system and to add more features to find novel attacks.

REFERENCES

[1] Nirnay Ghosh., S. K. Ghosh . :An Approach for Security Assessment of Network Configurations using Attack Graph In First International Conference on Networks & Communications(2009).

[2] Balzarotti, D., Monga, M., Sicari S.: Assessing the risk of using vulnerable components. In: Proceedings of the 1st Workshop on Quality of Protection (2005)

[3] L. Wang, A. Singhal, and S. Jajodia. : Measuring the overall security of network configurations using attack graphs. In Proceedings of the 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec), July 2007

[4] Nirnay Ghosh, S. K. Ghosh. :An Intelligent Technique for Generating Minimal Attack Graph. In proceedings of the 21st annual computer security applications conference(ACSAC 2005)

[5] L. Wang, T. Islam, T. Long, A. Singhal, and S. Jajodia. : An attack graph-based probabilistic security metric. In Proceedings of the International Federation for Information Processing (IFIP 2008).

[6] M. Schiffman : Common vulnerability scoring system (cvss).In journal National Infrastructure Advisory Council (NIAC) (2004)

[7] Pankaj Gupta and Nick McKeown. :Packet Classification using Hierarchical Intelligent Cuttings In Proceedings of Hot Interconnects (1999)

[8] Yaxuan Qi, Jun Li. : Performance Evaluation and Implementation of Algorithmic Approaches for Packet Classification

[9] Tito Waluyo Purboyo and Kuspriyanto. : Some Algorithms for Generating Attack Graph. In International Journal of Advanced Research in Computer Science and Software Engineering.Volume 2, Issue 8, August 2012

[10] Yinqian Zhang, Xun Fan, Yijun Wang, Zhi Xue. : Attack Grammer-A New Approach to Modeling and Analyzing Network Attack Sequences. In Annual Computer Security Applications Conference (2008)*Note that the journal title, volume number and issue number are set in italics.*