International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 2, Issue 3 (May-June 2014), PP. 158-162

NSAS: NETWORK SECURITY AWARENESS SYSTEM

Bhushan Khandelwal, Kapil Misar, Vinay Jain, Ravindra Kadagoudar
BE Computer Science.
SCOE Sudumbare
Pune, India

***Abstract* — The overwhelming threat may be a challenge to general security system. Fundamentally diverse alert and threat techniques are been researched in order to reduce deceptive warnings. Threat Detection Systems generates huge amount of alerts which becomes challenging to deal with them and prepare solution. The detection System checks inbound and outbound network activities and finds an suspicious pattern that indicate an ongoing steps for attack. Large amount of alert may contain false alarm therefore need of alert analysis mechanisms to offer high level information of seriousness of threat, how dangerous device are and which device admin has to pay more attention. To solve this query we would make use of time and space based alert analysis technique that provides a solution in form of attack graph and its evaluation that provides severity of attack to administrator.**

***Index Terms*— Alert, Alert pair, Unit Threat Evaluation, Attack Threat Evaluation, Network Threat Evaluation, Device Threat Evaluation Attack Graph.**

I. INTRODUCTION

Ever increasing use of the world wide web by various types of firms, companies, security threats such as attacks by hackers on enterprise infrastructure, the leakage of personal confidential representation of facts and the infection of secret business data caused by e-mail based viruses, have become major cause in the security literature over the last few decades. Security systems such as IDS i.e Intrusion Detection Systems and Firewalls have been developed to detect and protect these systems in wired and wireless networks. Intrusion detection systems are most of the time deployed along with other preventive and protective mechanisms, such as access control and authentication, as a second line of defense that secures information systems. In early days, developing application and systems were major concerns rather than security. There are distinct reasons that make intrusion detection a necessary part of the entire defense system. Nowadays, we face to overwhelming information which is mixed up and out-of-order and really hard to determine such useful Knowledge from such huge amount of information. The Situation Awareness is proposed to solve this kind of problem.

II LITERATURE SURVEY

Several modules have been proposed by the researcher which is used to analyze the attacks. The analysis, which can scan sessions and protocols that provides a abstract understanding of a network's architecture along with behavior. This ability can be used to identify network actions that cannot be understood from within session analysis or packet analysis only.. It is also used to supports larger, time-domain descriptions having similar network characteristics such as flow of packets, amount of traffic (data) sent, etc. In the last fifteen years the application of situational awareness (SA) has been revolutionary, particularly in air target control (ATC), defense space and cognitive science where SA has been extensively researched. Unfortunately, when compared to ATC or defense space, situational awareness in computer network security is still in its early stages. In computer networks, cyber-attacks are numerous and evolving, such as code-driven attacks, deliberate malicious software attacks, espionage, distributed denial of service attacks, phishing and insider attacks . A known fact is that the capability of any singular security control is limited. Unfortunately, it is not possible for organizations to purchase myriad security controls (for every type of attack perceived in the network), especially with the recent credit crunch, therefore, it has become ever more important for enterprise to seek alternative, accurate, reliable and affordable approaches. A recommended approach is to use existing controls in the organization but to combine their set of evidence to provide better situational awareness of network states, and interdependent risks that may exist in networks. Integrating evidence of existing security controls is the focus of multisource data fusion, where myriad heterogeneous security controls are combined to provide accurate situational awareness in the network. E.g., evidence of attacks perceived by firewalls, intrusion detection systems, security guards are all combined, such that their independent intelligence are aggregate to provide meaningful and richer inferences than that obtained from any individual security control. To observe (gather evidence), correlate and aggregate data from multiple observing sensors or persons to provide accurate and much improved decision of the observed phenomenon (situation) is the underlying building block of network security situational awareness.

III. PROPOSED SYSTEM

The current computer infrastructure can be easily infected to malicious activities, intrusion detection much need be its security is insufficient. Effective design is much need to circumvent intrusion when they are detected. Proposed method works on library that implements various types of threat counter measures and creates alert pairs and graphs. Proposed system aims to design a tool that helps the administrator to choose the suitable countermeasure when the intrusion occurs. For this purpose, we make use of alert pair algorithm to generate alert pair graph which determines the counter measures that are used to stop intrusions. Security systems like firewall, Intrusion detection system and security scanner independently work on the threats and are not designed to offer an threat evaluation techniques which make a challenging job for system administrator to analyze how critical the attack might be. Evaluation techniques like UTE – Unit threat evaluation that deals with the number of threats per unit in the network is calculated and threat evaluation solutions is provided, DTE – Device Threat Evaluation determines the threats affecting the network shared Devices (like printers), NTE – Network Threat evaluation deals with number of threats whole network, Lastly ATE – Attack Threat Evaluation is to determine the attacks in the whole network. To end with, we present the platform of intrusion detection, called NSAS that implement the response mechanisms presented in this paper.

MAJOR INSPIRATION

Firewall prevents the unauthorized users to access the data and sometimes are restrictive for performing legitimate operations. Whenever there chunks of data transmitted through database it may affect firewall security and can be easily breaked. Firewalls only blocks unauthorized data transmissions and don't provide anti-malware, anti-virus or anti-spyware capabilities, so we will need additional security to the system if this offensive software is accidentally introduced into that system. To overcome such threat we formed barrier which will act as a security guard. NSAS which is been developed to overcome this drawbacks uses algorithms like TSRA to restrict attacks. TSRA requires alert objects, an alert object is created when two or more requests are received by the server within an specific time window.

IV. PROPOSED METHODOLOGY

Main aim of our project is to build such a security which helps in creating an awareness of how much hazardous the threat is. This mainly will help admin offer intuitionistic information about the seriousness of that attack. It then suggest a high level security prospect based on the security alert actions. It will then reveal notification and detection of malicious packets within range. Creating such an awareness then will highly reduce the spurious positive and fake negative rates.

The approach of this project is to develop a NSAS combines and analyzes security alert actions collected from high level security situation sensors. It then will generate the network protective situation by extracting the often occurring and sequential patterns from the dataset of security circumstances based upon Knowledge research method and modify such patterns to the interrelation protocols of that network security condition and finally it will automatically provide the better network security situation graph. By this we are generally capturing the data from the network source which are dynamic in nature. This data may be consisting of source and destination IP which will be helpful in finding their path.

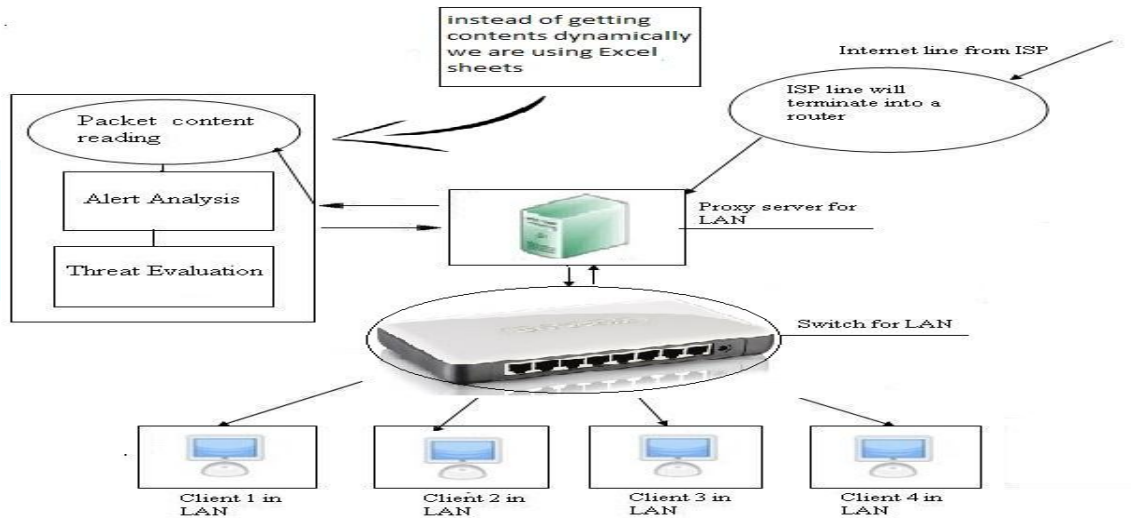

Fig Proposed_methodology: Network Diagram

Thus alert analysis technique would be made in use by ensuring and creating the alert pair .Once alert pairs are being made then correlation of such isolated alerts and alert pairs are being done. This will help in determining the false and true alarms. After the correlation being generated it is then converted to alert graph by using attack graph algorithm. Thus system architectural view are being made in case of such an alert pair and alert graph. Also some alert evaluation techniques like DTE, ATE, UTE, NTE are being processed.

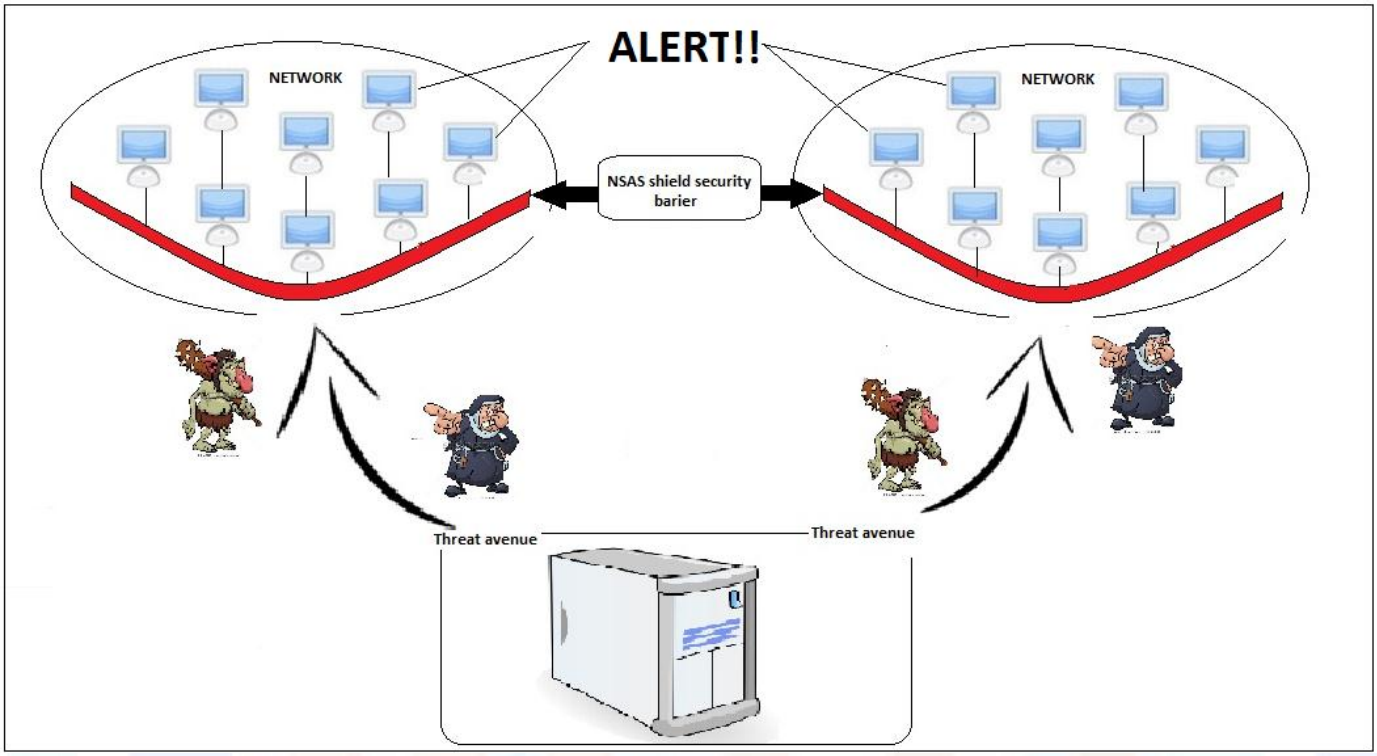

Fig:Proposed_Methodology:Proposed project

In this system we proposing basically threat avenue and how it approaches to our network system is being revealed. All the networks are having their firewalls which helps in restraining the threats evolving. But not all of the threats are being captured and neither many of such threats can be handled in an appropriate way. So beyond the server systems of our network we are placing the NSAS barrier. NSAS will act as a barrier for the threats and the attacks which are approaching towards the network systems. Whenever such threats like dos, sad mind , lldos are been approaching in bulk towards the system , it will create an awareness to the internal users. An alertness of such an abnormal activity been approached to the network system would help the users to be awared of it and a necessary action to be performed will be considered. Creating such an awareness will be very helpful to take necessary charge against the threats.

Based on Time and Space, we put forward an alert analysis technique which will correlate similar type alerts without having past knowledge and hence present an attack graph that provides the admin to identify the attack procedure clearly and efficiently. Thus a threat evaluation technique is given to find the most severe attack, which further saves administrator's time and effort in undergoing large amount alerts.

We propose our own strategy to spontaneously relate the alerts to provide an attack graph which depends on Time and Space restriction. Also, we include an attack evaluation technique. Initially we propose our own alert analysis way to correlate related alerts and offer an attack graph. Then an evaluation function for possible attacks (devices or on attack), with respect to these proposed methods, administrators can be able to identify the network situation and understand how severe an attack would be without checking particular alerts or evaluation values. Here NSAS just wants to find when, where and how much is the severity of an attack , so we need a subset of alert fields. Small alert message also saves much time and storage space.

DEFINITION 1.Alert: An alert *a* is a seven tuple (al_aid; al_srcip; al_dstip; al_srcport; al_dstport;al_ type; al_time):

- **al_aid** is an AUTO INCREMENT integer generated by database. It is used to identify each alert.
- **al_srcip** represents the source IP address. The operation Srcip(x) means get the source IP address of the alert a.

- **al_dstip** represents the destination IP address, the corresponding operation is Dstip(x).
- **al_srcport** represents the source port, the corresponding operation is Srcport(x)
- **al_dstport** represents the destination port, the corresponding operation is Dstport(x).
- **al_type** represents the alert's type, it is a short string which give a simple description of the attack, the corresponding operation is Type(x).
- **al_time** represents time of the alert generate, the corresponding operation is Time(x).

V. Time And Space Restriction Analysis (TSRA)

To perform attack successful several steps are involved. Initially attacker may uses the scan tools to get the target network information. After determining the vulnerabilities of the network, the attacker will concentrate on certain devices, and start to execute attack actions. These attack steps are interrelated, and hence their corresponding alerts are also related. Basically we correlate the similar type alerts to an attack scenario based on TSRA. Two alerts xi, xj, if they are similar, then usually we have some time and space relations as listed below:

1. Srcip(xi)=Srcip(xj), Dstip(xi)=Dstip(xj), Time(xi) <Time(xj).
2. Dstip(xi)= Srcip(xj), Time(xi) <Time(xj).

The above two conditions are used to generate an alert pairs. In initial stage, if source ip of alert xi is same as that of source ip of xj, Destination ip of alert xi is same as of Destination ip of xj such that time of xi is less than that of xj. In second condition destination ip of xi should be same as that of source ip of xj and time of xi should be less than time of xj then add the hyper-alerts to alert pair.

Algorithm 1 describes the way of correlating two or more isolated alerts to alert-pair.

Algorithm 1: Correlation of Isolated Alert to Alert-pair:

Input: individual hyper-alerts x1,x2……xn

Output: set of alert-pairs (xi,xj). denoted Alert Pairs.

Let ap_TW be the time-window which is set by administrators.

1. for all the hyper alert in hyperalert do
2. if Srcip(xi) = Srcip(xj) and Dstip(xi) = Dstip(xj) and Time(xi) <Time(xj) and Time(xj) – Time(xi) < ap_TW Then
3. put (xi,xj) into Alert-Pairs.
4. if Dstip(xi) = Srcip(xj) and Time(xi) < Time(xj) and Time(xj) – Time(xi) < TW Then
5. Insert (xi,xj) into Alert-Pairs.

Thus atlast we correlate such alert pairs to the as giving in next attack graph generation Algorithm 2

Algorithm2 : Algorithm to generate attack graph.

Input :set of alert-pair (xi,xj) - APs.

Output: attack graph G(Nd,Ed)

Put every hyper-alert xi of APs into node set Nd;

Put every alert-pair (xi,xj) of APs into edge set Ed;

1. for every edge(ndi,ndj) do
2. if there is a indirect path ndi,…..,ndk,….ndj then
3. remove the edge (ndi, ndj) from edge set Ed
4. return G(Nd,Ed)

VI. EVALUATION TECHNIQUES

1) Unit Threat Evaluation

Evaluation of Number of Threats attacking per unit in an network is Unit Threat evaluation.

$$E_{ad} = 10^{l(a)-1} * 10^{l(d)-1}$$

where,

$\mathbf{E_{ad}}$ - Unit Threat Evalution

l(a) - level of the alert

l(d) - level of device

2) Attack threat evaluation(ATE)

Each device that is intruded with a unit evaluating value and sum of that device values UTE of that attack is ATE.

$$\mathbf{E_a} = \sum_{i=1}^{m} \mathbf{E_{adi}}$$

where,

$\mathbf{E_a}$-attack threat evaluation

$\mathbf{E_{adi}}$-unit evaluation value

3) Device threat Evaluation(DTE)

Device when attacked by various attacks, each attack make a unit threat for such device also sum of that unit threat is the complete threat i.e device threat.

$$E_d = \sum_{j=1}^{n} E_{ajd}$$

where,

$\mathbf{E_d}$-device threat

$\mathbf{E_{ajd}}$-unit threat

4) Network threat evaluation(NTE)

Network when attacked by sum of threat value of each attack.

$$E_N = \sum_{j=1}^{n} E_{aj}$$

where,

$\mathbf{E_N}$-network threat

$\mathbf{E_{aj}}$-threat value

Behaviour of each and every incoming packet is analyzed which reveals the severity and type of attack like DOS, DDOS and thus offers attack graph which is helpful for preventive measure of attacks. These information are used by administrator so that he may manage ip, block unwanted request from client that prevents attacks like DOS,DDOS.

Attack graph demonstrates the no of requests on the device. The nodes 1,2,3,4,5 are the devices in the network, also c1 is internal user &c2,c3 are external to the network. In fig the node 3 is the server node which takes in request from various clients. The edges represents the path of attack from client to the devices in the network. Also the graph shows number of request from internal users and external users clearly. Graph is helpful to understand the nature and strategy of attack including the path followed. Graphical representation illustrates the attack done on the network throughout a defined timestamp.

VII. RESULTS AND DISCUSSIONS

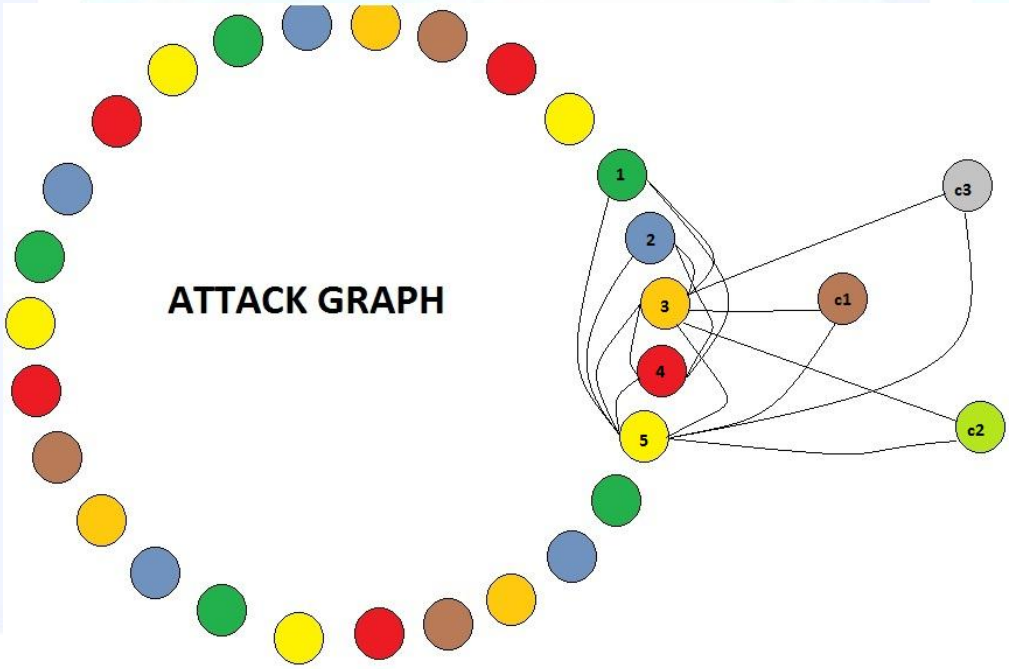

Fig :Results_and_Discussion: Attack_graph

VIII. ACKNOWLEDGMENTS

Our sincere thanks go to Siddhant College of Engineering for providing a strong platform to develop our skill and capabilities. We would like to thanks to our friends,& relatives for their constant support and motivation for us. Last but not least, we would like to thanks all those who directly or indirectly help us in presenting the paper.

IX. REFERENCES

[1] A. H. Debar, "The intrusion-detection console correlation mechanism" , In 4th International Symposium on Recent dvances in Intrusion Detection(RAID), 2001.

[2] M. L. Laboratory, 2000 DARPA intrusion detection scenario specific data sets,http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/2000data.html (2000).

[3] B. Mica R.Endsley, Bolte, C. Jones, D., Designing for situation awareness: An approach to user-centered design, Taylor and Francis,
2003.

[4] P. Ning, Y. Cui, D. S. Reeves, D. Xu, Techniques and tools for analyzing intrusion alerts, ACM Trans. Inf. Syst. Secur. 7 (2) (2004) 274–318.

[5] D. X. Peng Ning, Learning attack strategies from intrusion alerts, in:CCS '03: Proceedings of the 10th ACM conference on Computer and communications security, ACM, New York, NY, USA, 2003.

[6] X. Qin, W. Lee, Attack plan recognition and prediction using causal networks, in: ACSAC '04: Proceedings of the 20th Annual Computer Security Applications Conference, IEEE Computer Society, Washington, DC, USA, 2004.
[7] Snort, http://www.snort.org/.

[8] I. S. Systems, Realsecure intrusion detection system, http://www.iss.net.

[9] C. Xiuzhen, Z. Qinghua, G. Xiaohong, L. Chenguang, Study on evaluation for security situation of networked systems, JOURNAL OF XIAN J IAOTONG UNIVERSITY, Vol. 4, 2004, 76-80.