ISSN:2320-0790

An International Journal of Advanced Computer Technology

Uniform Comparison Approach for Different Network security Assessment Using HRCAL Method

Ankita Patil[1], Vijay Prakash[2]

[1]Research Scholar, Dept. of CSE, SVITS, Indore, (M.P), India

[2]Associate Prof., Dept. of CSE, SVITS, Indore (M.P), India

ABSTRACT: Network security the field of network security is very dynamic, and highly technical field dealing with all aspects of scanning, hacking and securing system against intrusion. And we know that today's the attacks on internet is major issue, today's world of technology the fault security is becoming an almost incurable problem in today's network. For these attacks Here we provide the situation awareness mechanism to know about the situation of network and let them aware from situation of network. In my previous work, I had provided the situation awareness mechanism that gather the network actual condition and clearly define the boundaries by which security solution can be made and I had also gone to detect network condition and draw the graphs with the help of security metrics. In this paper I am going to compared my proposed work with other work.

KEY WORDS: Situation Awareness (SAM), Vulnerability, Attack Graphs, Network Configuration Metrics, HRCAL (Host, Route, Configuration and Attack Level Analysis).

1. INTRODUCTION

Network security consists of the provision, policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Network security starts with authenticating, commonly with a username and a password. Since this requires just one detail authenticating the user name i.e. the password this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used. At present, the network constitutes as a core component for information processing system in various areas like financial sector, power generations and emergency systems. For these here we introduce the SAM. The idea behind the network security situation assessment and awareness is for consolidation of all available information for identification of attack vulnerable to the system.In this process it works as a decision making method which has the prediction of attack vulnerability on a selected device. Thus, this method it's measured analytically that the attack vulnerability are going to be detected additional accurately in real time. Here the protection scenario of current communication and networked operations are analyzed on the premise of previous participation's and vulnerability measuring. For proving the usefulness of the approach a dummy attack is generated and inserted during this system. Existing approaches had situation-awareness consist of vulnerability analysis using attack graphs, intrusion recognition and alert association, attack analysis, attack impact analysis and forensics and information flow analysis. Based on the fusion of network information, the current tools make a qualitative assessment on the situations of network security.

2. RELATED STUDY

The security metrics based mostly network situational awareness methodology is being prompt to facilitate the decision making. It is being applied for the advance of associate existing configuration by police work the changes within the type of data and behaviour of devices. The approach is grouping numerous records and processed them for reporting the relevant performance factors using a quantitative approach. The strategies also are capable of dominant the operation by exploitation some extra parameters of adequacy analysis of security method enhancements. A number of approach conjointly suggests passive mechanisms based mostly observance tools for finding out the network requirements and named as Panemoto (Passive Network observance Tool) [2].In the paper[3] , it is calculated with the help of visualization mechanism for correct assessment like that form attack graphs. It provides potential and accurate mechanism using model based on Gray Theory through Residual Error

Corrections. It uses three functions Primary residual error correction, secondary residual error correction, and tertiary residual error correction. It resolves the issues related to discrete nature of raw data. Although the proposed method has done some research in achieving network security situational awareness, but many of the key issues needs to be deepen and improved. The experimental evaluation shows that the observation of the model to the network security situation is able to achieve a reasonable getting accuracy, which is full of practical terms. In the paper[4], author suggested a novel framework for security evaluation with attack modeling using SIEM (Security Information and Event Management) system. It is totally based on internet data for better analysis of security situations and current attack involvements. The proposed management system is based on attack analysis using malefactor behaviour identification and graph generation through various metrics for risk assessment. The paper also presented a prototype for future implementation based on suggested approach. Primarily it is calculating the vulnerability using interactive decisions. The precise and real-time forecast of network protection state of affairs is that the foundation and basis of preventing intrusions and attack in an exceedingly intensive network. In categorization to expect the safety condition a lot of accurately, a quantitative calculation methodology of advanced security condition based on Wavelet Neural Network with Genetic Algorithm (GAWNN) is proposed in. When analyzing the past and therefore the recent network security condition thoroughly, it builds a network security state of affairs prediction model supported a Wavelet Neural Network that's optimized by the improved genetic algorithmic and then adopt GAWNN to predict the non-linear time series statistic of the network security state of affairs. When analyzing numerous simulation experiments, it proves that the planned methodology has blessings over Wavelet Neural Network (WNN) methodology and Back Propagation Neural Network (BPNN) methodology with an equivalent design in convergence speed, functional approximation and prediction accuracy. In the paper , the author introduces the tools and techniques used to store information about sequences of packets as they are collected on an enterprise network for SiLK. It gives the result approximation based on network flows by generating its own records for data transmission. It analyses multiple flow records for situation assessment. Mainly it identifies active timeout, cache flush and router exhaustion for attack analysis and vulnerability assessment. So by giving both the volume and complexity of this data, it is critical to understand how this data is recorded and that is effectively achieved by above visualization tool. The above study on various research articles demonstrates here that how actual assessment of network is required to be for removal of deficiencies of existing systems. So the derived results shows that using common vulnerability standards is not sufficient apart form that some more data mapping metrics needs to be used and a new model needs to be proposed for effective detections.

3. PROBLEM DOMAIN

Network situation security assessment and awareness is mechanism which requires frequent modifications in attack databases and must give real time vulnerability calculations and alerts. It is used to perceive network security situations comprehensively. Based on the fusion of network information, the current tools make a qualitative assessment on the situations of network security. The existing system can recognize the network security situations through fusing large amount of network information. The existing system which is taken as a base for this work CNSSA [1] adopts the measurement metrics of the Common Vulnerability Scoring System (CVSS) to make quantitative assessment on the situations of network security which needs to be modified for frequent updates processing. It should also implements filter function in its information collection process. To measure the overall security of a network one must first understand the vulnerabilities and how they can be combined to construct an attack. Recent advances using attack graphs can be used to measure quantitatively the security of a network.

4. SYSTEM DOMAIN

The prime aim of this proposed dissertation domain is to increase the security level of the system through assessing the current situation through situation awareness phenomenon. This work measures the network situation through various assessment metrics and applies the most suitable approach to reduce the vulnerability through various assessed attacks. The proposed work had stored the network state while there is no attack probability and then continuously monitors the current state. Comparison is made regularly to detect the attack probability through the attack graphs. It measures the type of changes occurring in the network and detect potentially anomalous changes to the network configuration. This potential can alert administrators to dynamic changes in the network situation. It detects the devices and networks that are new, missing, or changed, and displays their information depending on their status. It expresses the value on behalf of two measurable metrics:

a) Qualitative Assessment (Risk analysis).
b) Quantitative Computation Network Security (Bayesian sets and fuzzy theory).

The real situation awareness mechanism automatically analyze huge amount of data for useful patterns, unusual behavioral and configuration changes, measuring the dependencies in effective manner. It involves data extraction techniques like spatial index, predictive analytics and machine learning to take the decisions. To measure such awareness security metrics is a very important aspect for information security. These metrics are to facilitate decision making and improves performance accountability. It ensures business value continuity and reduces business losses by preventing and minimizing the impact of security reports. Thus security must contain the complete structure of the organizations information security and risk handling process. It represents all the parameters in quantifiable and measurable manner. They have to be considered as a reference point which allows the admiration of the systems quality points. This term is very often used to describe the concepts of metric, measure, score, rating, rank or assessment. But for the most important objective of the information security metrics is being developed and specify a useful decision support reporting security system.

5. PROPOSED WORK

The proposed architecture of the system is shown in figure 1.1. Initially the number of system is monitored to get the current network situation values. Under this monitoring phase various types of network devices and their status is sensed like it will detect the changes occurring in the network configurations, number of host variations, devices working efficiency etc. This measured data is stored in the repository store for current state values. It consists of two stages: security policy detection and network configuration assessment. In the next phase this information can be read by information collector modules from the log details of the individual store and repository for respective data. This data is then passed on to situation measurement modules which work on the bases of five metrics: network configuration, attack impact, policy updates, attack routes and threat risk analysis. This metrics is used for awareness generation regarding the current network situation and for malicious and unwanted activity pattern detection.

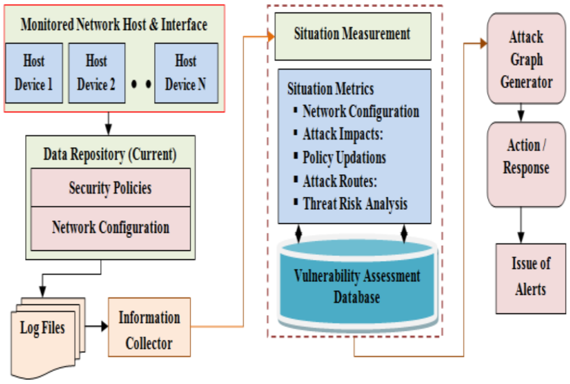


Figure 1.1: HRCAL Based Network Situation Awareness

This can be achieved by creating various attack graphs from which decision can be taken to detect such activities. Thus an attack graph created from the suggested metrics is going to calculate the types of response and action identification. This mechanism will also generate the alert message to aware the system admin or the controlling device to stop such activity. In this way an improved network awareness can be identify to measure to improve the existing network security situations based on Host, Route, Configuration and Attack level analysis (HRCAL).

6. PERFORMANCE AND COMPARISON

Table: Table 1. table for suggested HRCAL

S.No	Name	Functionality/Type of metrics	Data Source
1	Host Behaviour	Type,Specification,Criticality Level	Scan Information
2	Attack Routes	Response time, Dealt, Route Length, Max & Min Damage Route	Network Traffic
3	Network Configuration	Network Bandwidth Consumption	Network Traffic
4	Attack Impact	Packet Drop Rate, Damage Level, Vulnerability, Score	IDS Alerts
5	Threat Level	Min and Max quality of different vulnerable, Risk level of threat	DS Alerts

Data to be used for paper: Situation mindfulness is vital for enhancing the security of system having substantial number of gadgets constantly collaborating with every others. It is connected with different application like military, medical service, aviation authority or flight’s and so on. On other hand, the quality of studies in the field of situation mindfulness for new applications has become fundamentally in the recent years. System security circumstance mindfulness framework ought to can deal with data originating from different source, which will incorporate data of system topology, system arrangement, vulnerabilities, framework logs, system security gadget caution, system activity and so on.In light of legitimate data combination, a system security circumstance mindfulness framework gives system expert knowledge into security important exercises happening inside their system, to help them settle on choices or alterations on their systems. Along these lines as its utilization is expanding the trust for more exact as assault investigation is additionally making weight. Subsequently for giving a turn in the zone of security appraisals, this work proposed a novel HRCAL security circumstance mindfulness system focused around five set of measurements. The remarkable gimmick of the proposed framework is constant investigation and conduct plotting through assault diagrams. It can likewise process different sort of data at the same time. At the beginning level of exploration it demonstrates as a superior choice for system and security overseer. Future results and usage model will doubtlessly makes the route open for different analyst.

Expected Benefits

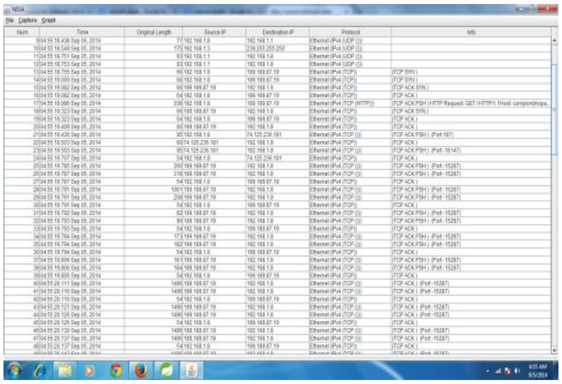
The given methodology contrasts from the previous work in that it concentrates on attenting to complete and precise risk assessment. The genuine circumstance mindfulness instruments consequently examine immense measure of information for valuable example, unordinary behavioral and design changes, measuring the conditions in powerful way. As opposed to accentuating especially the effect of disengaged occurrences, the current instrument of HRCAL channels out same system parcels relating to unimportant or invalid interrupting by melding data (administration, application programming and powerlessness) created by a scanner, and a few bundles comparing to unsuccessful interruption by utilization of interruption reaction decides that serve as the standard for figuring out if or not it is to succeed in attaining to client benefit. When a choice is arrived at, arranging and execution (of the reaction activities) happen.

1. Better Security analysis process;
2. Easy modification of network configuration and security policy.
3. Attacker behavior and intent analysis
4. Information combination for network situation-awareness
5. Achieving self-awareness for network devices
6. Active and passive attack detection
7. Transmission intrusion detection
8. Deep Packet Inspection

7. RESULT EVALUATION

7.1 Logging table:

This table provides the uniform approach for data enter in the network with information about time,Source IP,Destination IP,Server information all this field comes under this table approach.

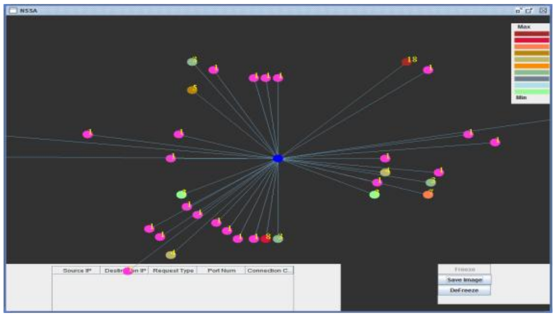


Num	Time	Original Length	Source IP	Destination IP	Protocol	Info
9	04:55:18.438 Sep 05, 2014	77	192.168.1.8	192.168.1.1	Ethernet (IPv4 (UDP ()))	
10	04:55:18.549 Sep 05, 2014	175	192.168.1.3	239.255.255.250	Ethernet (IPv4 (UDP ()))	
11	04:55:18.751 Sep 05, 2014	93	192.168.1.1	192.168.1.8	Ethernet (IPv4 (UDP ()))	
12	04:55:18.753 Sep 05, 2014	93	192.168.1.1	192.168.1.8	Ethernet (IPv4 (UDP ()))	
13	04:55:18.755 Sep 05, 2014	66	192.168.1.8	199.189.87.19	Ethernet (IPv4 (TCP))	(TCP SYN)
14	04:55:19.000 Sep 05, 2014	66	192.168.1.8	199.189.87.19	Ethernet (IPv4 (TCP))	(TCP SYN)
15	04:55:19.082 Sep 05, 2014	66	199.189.87.19	192.168.1.8	Ethernet (IPv4 (TCP))	(TCP ACK SYN)
16	04:55:19.082 Sep 05, 2014	54	192.168.1.8	199.189.87.19	Ethernet (IPv4 (TCP))	(TCP ACK)
17	04:55:19.086 Sep 05, 2014	338	192.168.1.8	199.189.87.19	Ethernet (IPv4 (TCP (HTTP)))	(TCP ACK PSH) HTTP Request: GET / HTTP/1.1Host: camplonbhopa...
18	04:55:19.323 Sep 05, 2014	66	199.189.87.19	192.168.1.8	Ethernet (IPv4 (TCP))	(TCP ACK SYN)
19	04:55:19.323 Sep 05, 2014	54	192.168.1.8	199.189.87.19	Ethernet (IPv4 (TCP))	(TCP ACK)
20	04:55:19.409 Sep 05, 2014	60	199.189.87.19	192.168.1.8	Ethernet (IPv4 (TCP))	(TCP ACK)
21	04:55:19.436 Sep 05, 2014	95	192.168.1.8	74.125.236.181	Ethernet (IPv4 (TCP ()))	(TCP ACK PSH) (Port 187)
22	04:55:19.503 Sep 05, 2014	60	74.125.236.181	192.168.1.8	Ethernet (IPv4 (TCP))	(TCP ACK)
23	04:55:19.503 Sep 05, 2014	95	74.125.236.181	192.168.1.8	Ethernet (IPv4 (TCP ()))	(TCP ACK PSH) (Port-18147)
24	04:55:19.707 Sep 05, 2014	54	192.168.1.8	74.125.236.181	Ethernet (IPv4 (TCP))	(TCP ACK)
25	04:55:19.785 Sep 05, 2014	260	199.189.87.19	192.168.1.8	Ethernet (IPv4 (TCP ()))	(TCP ACK PSH) (Port-15287)
26	04:55:19.787 Sep 05, 2014	318	199.189.87.19	192.168.1.8	Ethernet (IPv4 (TCP ()))	(TCP ACK PSH) (Port-15287)
27	04:55:19.787 Sep 05, 2014	54	192.168.1.8	199.189.87.19	Ethernet (IPv4 (TCP))	(TCP ACK)
28	04:55:19.791 Sep 05, 2014	1061	199.189.87.19	192.168.1.8	Ethernet (IPv4 (TCP ()))	(TCP ACK PSH) (Port-15287)
29	04:55:19.791 Sep 05, 2014	208	199.189.87.19	192.168.1.8	Ethernet (IPv4 (TCP ()))	(TCP ACK PSH) (Port-15287)
30	04:55:19.791 Sep 05, 2014	54	192.168.1.8	199.189.87.19	Ethernet (IPv4 (TCP))	(TCP ACK)
31	04:55:19.792 Sep 05, 2014	82	199.189.87.19	192.168.1.8	Ethernet (IPv4 (TCP ()))	(TCP ACK PSH) (Port-15287)
32	04:55:19.793 Sep 05, 2014	90	199.189.87.19	192.168.1.8	Ethernet (IPv4 (TCP ()))	(TCP ACK PSH) (Port-15287)
33	04:55:19.793 Sep 05, 2014	54	192.168.1.8	199.189.87.19	Ethernet (IPv4 (TCP))	(TCP ACK)
34	04:55:19.794 Sep 05, 2014	173	199.189.87.19	192.168.1.8	Ethernet (IPv4 (TCP ()))	(TCP ACK PSH) (Port-15287)
35	04:55:19.794 Sep 05, 2014	192	199.189.87.19	192.168.1.8	Ethernet (IPv4 (TCP ()))	(TCP ACK PSH) (Port-15287)
36	04:55:19.794 Sep 05, 2014	54	192.168.1.8	199.189.87.19	Ethernet (IPv4 (TCP))	(TCP ACK)
37	04:55:19.806 Sep 05, 2014	161	199.189.87.19	192.168.1.8	Ethernet (IPv4 (TCP ()))	(TCP ACK PSH) (Port-15287)
38	04:55:19.806 Sep 05, 2014	184	199.189.87.19	192.168.1.8	Ethernet (IPv4 (TCP ()))	(TCP ACK PSH) (Port-15287)
39	04:55:19.806 Sep 05, 2014	54	192.168.1.8	199.189.87.19	Ethernet (IPv4 (TCP))	(TCP ACK)
40	04:55:20.111 Sep 05, 2014	1496	199.189.87.19	192.168.1.8	Ethernet (IPv4 (TCP ()))	(TCP ACK) (Port-15287)
41	04:55:20.116 Sep 05, 2014	1496	199.189.87.19	192.168.1.8	Ethernet (IPv4 (TCP ()))	(TCP ACK) (Port-15287)
42	04:55:20.116 Sep 05, 2014	54	192.168.1.8	199.189.87.19	Ethernet (IPv4 (TCP))	(TCP ACK)
43	04:55:20.121 Sep 05, 2014	1496	199.189.87.19	192.168.1.8	Ethernet (IPv4 (TCP ()))	(TCP ACK) (Port-15287)
44	04:55:20.126 Sep 05, 2014	1496	199.189.87.19	192.168.1.8	Ethernet (IPv4 (TCP ()))	(TCP ACK) (Port-15287)
45	04:55:20.126 Sep 05, 2014	54	192.168.1.8	199.189.87.19	Ethernet (IPv4 (TCP))	(TCP ACK)
46	04:55:20.132 Sep 05, 2014	1496	199.189.87.19	192.168.1.8	Ethernet (IPv4 (TCP ()))	(TCP ACK) (Port-15287)
47	04:55:20.137 Sep 05, 2014	1496	199.189.87.19	192.168.1.8	Ethernet (IPv4 (TCP ()))	(TCP ACK) (Port-15287)
48	04:55:20.137 Sep 05, 2014	54	192.168.1.8	199.189.87.19	Ethernet (IPv4 (TCP))	(TCP ACK)

Logging network detail

7.2 Network graph Description:

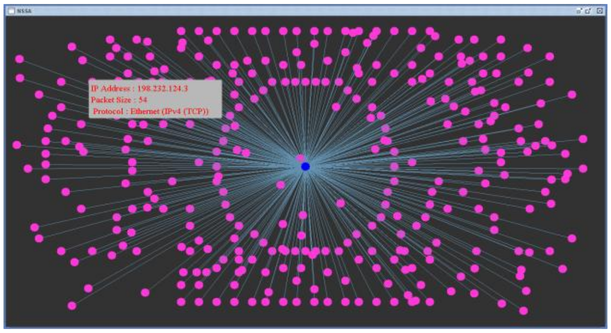
In this graph it shows a central node pointed blue can be connected with different node in a uniform manner, different nodes represented by pink dots



Network graph with different colour

7.3 Node detail graph:

This graph shows details of different nodes in a loop,it provides information on IP Address from where it originated,it also provides information about the packet size and on which protocol it is based



IP Address : 198.232.124.3
Packet Size : 54
Protocol : Ethernet (IPv4 (TCP))

Node detail graph

7.4 Showing Node detail Saved:

In this graph it shows details of different nodes and saved the image on the basis of node location

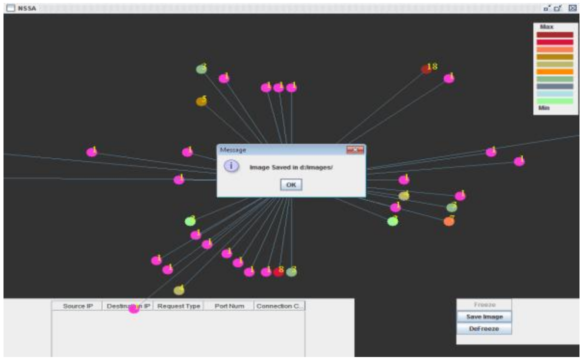


Image Saved in d:/images/

8. CONCLUSION

In the present era computer network is taken as the core component of various technology supported areas such as banking sector, emergency systems and communication areas. With this increase in network usage the kind of data protection required to make the system secure is also serving as a challenging task. It includes attack resistant Internet services which results high demand for network analyst which measures the security situations successfully. Existing network analysis tools lacks such capabilities of analyzing the network and access situations correctly. Situation awareness mechanism gathers current network condition and clearly defines the boundaries by which security solutions can be designed effectively. In this research paper I have compared my research work with other research.

ACKNOWLEDGMENT

This research work is self financed but recommended from the institute so as to improve the HRCAL with current techniques in network security using this method. Thus, the authors thank the anonymous reviewers for their valuable remarks, which strengthened the paper. The authors also wish to acknowledge institute administration for their support & motivation during this research. They also like to give thanks to Mr. Vijay Prakash & Mr. Rajiv Vishwakarma for discussion regarding the situational awareness system & for producing the approach adapted for this paper.

REFERENCES

[1] Rongrong Xi, Shuyuan Jin, Xiaochun Yun and Yongzheng Zhang, “CNSSA: A Comprehensive Network Security Situation Awareness System”, in International Joint Conference of IEEE TrustCom, ISSN: 978-0-7695-4600-1/11, doi: 10.1109/TrustCom.2011.62, 2011.

[2] Yu Dong and Frincke, D. , "Alert Confidence Fusion in Intrusion Detection Systems with Extended Dempster-Shafer Theory, " 43rd ACM Southeast Conference, March 18-20, 2005.

[3] Rongzhen FAN, Mingkuai ZHOU, “Network Security Awareness and Tracking Method by GT”, in Journal of Computational Information Systems, Binary Information Press, ISSN: 1043-1050, Vol. 9: Issue 3, 2013.

[4] Igor Kotenko and Andrew Chechulim, “Attack Modelling and Security Evaluation in SIEM System”, in International Transaction of System Science and Application, SIWN Press,, ISSN:2051-5642, Vol. 8, Dec 2012.

[5] Lingyu Wang, Tania Islam, Tao Long, Anoop Singhal, and Sushil Jajodia, “An Attack Graph-Based Probabilistic Security Metric”, in National Institute of Standards and Technology Computer Security Division; Concordia Institute for Information Systems Engineering, Montreal, Canada.

[6] Marianne Swanson, Nadya Bartol, John Sabato, Joan Hash, and Laurie Graffo, “Security Metrics Guide for Information Technology Systems”, in NIST Special Publication 800-55, July 2003.

[7] Pallavi Vaidya and S. K. Shinde, “Application for Network Security Situation Awareness”, in International Conference in Recent Trends in Information Technology and Computer Science (ICRTITCS - 2012), IJCA, ISSN: 0975 – 8887, 2012.

[8] Ankita Patil, Vijay Prakash “A Novel Framework for Composite Network Security Situation Assessment Using HRCAL Approach” international journals of Engineering Science Research and Technology. Jun 10, 2014.

[9] Ankita Patil, Vijay Prakash “Performance Evaluation of Composite Network Security Situation Assessment Using HRCAL” international journals of Research in Computer Engineering and Electronics. Dec 26, 2014.