

Comparative Study of NSSA with Different Network Security Aspects

Miss. Ankita Patil,

Research scholar
Dept. name of CSE
SVITS, Sanver Road
Indore (M.P.), India
Ankitapatil1310@gmail.com

Mr. Vijay Prakash

Associate Prof.
Dept. name of CSE
SVITS, Sanver Road
Indore (M.P.), India
Vijayprakash15@gmail.com

Abstract

Network security is an organization strategy and provisions for ensuring the security of its assets and of all network traffic. At present, the network constitutes as a core component for information processing system in various areas like financial sector, power generations and emergency systems. These systems are continuously using different types of information's from multiple locations. This work is going to detect the actual network status by using various metrics of the basis of which accurate decisions can be made. These decisions are used for assessing the current network and status of working devices and let them aware about the network actual conditions. Primarily the HRCAL work is using four categories of metrics like Host, Route, Configuration and Attack Level Analysis. In this paper I have gave the comparative study of survey method according to their reliability, security, robustness, scalability and also shows the efficiency.

Index Terms— Vulnerability, Security, Stability, NSSA, Attack Graphs, Network Configuration Metrics, HRCAL (Host, Route, Configuration and Attack Level Analysis).

I. Introduction

Network security is a complicated subject. Network has been defined as any set of interlinking lines resembling a net, a network of roads an interconnected system, a network

International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 1, April 2015

alliances. These systems are continuously using different types of information's from multiple locations. In such situations where data is generating and getting updated regularly from various ends identifying its behaviour and authenticity is a critical area of work for researchers. Security of these networks from malicious intrusions is significant to the economy and of our people. Thus a standard way to measure network security will brings different users together with vendors and researchers. In the last few years there has been some significant improvements over providing standardizing such security measures using: Topological Vulnerability Analysis, Network Hardening and Attack Response. To provide the better security against the tremendous attacks in the Internet, there is developing high demand for network analysts to know about the situations of network security effectively [1]. The existing tool lacks such functionality of analyzing and representing the actual network behaviour. For each network and security, assumptions, the current focus is on qualitative aspects rather than a quantitative analysis. Thus, to measure the overall security of a network one must first understand the vulnerabilities and how they can be combined to construct an attack which is harmful for network. In this process it works as a decision making method which has the prediction of attack vulnerability on a selected device. The forecast shows that the attack pattern is totally matched by previously keep values and its impact is analysed. in line with known knowledge the choice ought to be taken to inform the other nodes, by Associate in alert message. Thus, by the on top of method it's measured analytically that the attack vulnerability are going to be detected additional accurately in real time. 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. Thus this work identifies such boundaries from which attack resistant system can be separated from actual changes by mapping those parameters on visualization mechanism. It uses metrics based measurement for achieving its goal in timely basis.

II. Related Study

It counsel a unique model SIEM (Security info and Event Management) for attack evaluations. The development measures the behaviour of existing attacks and therefore the generating nodes for correct analysis through a standard attack graph generator. It uses numerous security metrics for providing correct risk analysis throughout attack modelling security part (AMSEC) execution phase. The paper conjointly presents associate epitome model for result analysis[1]. The paper [2], 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. Apart from the above vulnerability identification mechanism there are some mechanism which is designed to identify the intruder's process and their affections. One of that is AIDF (analytical intrusion detection framework) which is proposed in [3]. It uses a probabilistic

International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 1, April 2015

inference mechanism for generating the most probable forensic clarification based on not only just the practical intrusion detection alerts, but also the unreported signature rules that are exposed in the possibility model. It is quite often for IDs to be opened in full logging mode for the forensic data gathering. It can be considered as practical implementation and solution of anti-DoS strategy in a authentic world deployment. So many authors had also worked on reducing the complexity so such systems which are too complex to implement for a smaller systems.

III. Problem Statement

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. The information processing is based on fusion of network factors and parameters which is used to make the preventive assessment of the situation. Aim is to detect the unusual patterns and from this predict the future affects of the attacks on mentioned devices. After studying the various existing approach in the different areas of the network used for predictions and forecasting, this work had identify that analyst have to know the patterns in a restricted manner and the detection is totally based on logical capabilities of few of those. Thus, some automation is required for better understanding of vulnerabilities and effects of attacks. Here are the some identified issues in existing approaches for resolving the issues of vulnerability analysis.

Problem 1: All the existing system will consider vulnerability in a qualitative aspect rather than some quantitative aspects which mislead the analyst's.

Problem 2: Real time measurement is not given by which losses are comparatively larger than others.

Problem 3: Massive data processing some time generates false alarm and incorrect predictions thus prediction accuracy needs to be considered as primary parameters for the work.

Problem 4: The assessment used to classify network state and the level of information required for optimal illustration is not complete always which misguide the prediction. Thus the transformation of such information with certain attributes is not provided by any of the existing mechanisms [2].

Pattern to be searched for in the network traffic graph can be specified as a subgraph in the DOT format. For example, to search for a denial of service attack pattern, one can specify a

International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 1, April 2015

graph where there are a number of nodes attacking (sending packets to) a single victim node around the same time. Note how one can specify various attributes in this specification. If a node or edge attribute matching is activated, the specified attributes are matched while finding patterns in the input graph. Enabling attribute matching provides a lot of flexibility in composing patterns. Attributes can be composed of the following types: string, position coordinates (pair of comma separated real numbers. Among them one is given in [4] for reducing the complexity of generating the attack graph. The suggested approach concludes the work as: First, it splits the network into fragments and does parallel computing for each fragment with subsequent result combinations and second, it gives the aggregation and abstraction for representations of attack actions. Its evaluation is based on comprehensive simulation of malefactor's actions, construction of attack graphs and computation of different security metrics. At the initial level of work, its experimental results show its authenticity and accuracy.

IV. Proposed System

This work proposes a novel HRCAL model for accessing the actual network situations and providing the attack resistant decisions on time. It increases the security views which are available with current networks. The work measures the actual network conditions by accessing the data from all the connected devices. It identifies the changes made in the network which are positive and which are making the network down. Hence making the system as anti-attack resistance, it needs to get better analysis of their behaviour and impacts levels. Thus it uses 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. Security is the means of achieving confidentiality and privacy with robust data transmission and availability. For effective communication over the network, it could be treated as critical factor and must be monitored continuously. Network is a big working environment made from collection of various devices, protocols, servers and host parallel generating thousands of records per unit time. Processing of such huge amount of data is a complicated task and requires more efforts in terms of time and cost. Thus, this paper provides an alternative way of handling security by vulnerability assessment. According to the approach, network components are analysed on their previous activities and changes accommodated. These factors should be permitted or rejected accordingly to their probability of attack vulnerable values called as assessment values .

Higher be the generated value larger be the attack occurrence probability and smaller be the value less probable to attack. Representation of component for this network pattern analysis based vulnerability measurement is given by attack graph. There are some benefits of using the metrics in this work given here as:

- 1) Improved performance and protection level of the system
- 2) Monitoring model which compares the current values with ideal values after which validation of operations and changes is measured.
- 3) Contribute to the enhancement of the existing security practices and to the integration of information security to its business processes values.

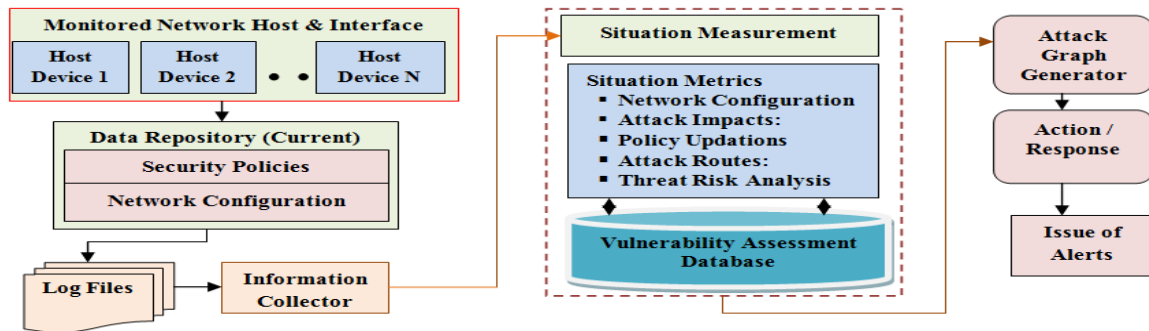


Fig.1. HRCAL based network situation awareness

Metrics Used

- *Metrics based on Network Configuration* (Quantity of Hosts, Firewalls, Type of Hosts, Hosts with Antivirus Software Installed, Hosts with Firewalls, Hosts with Host Based Intrusion Detection Systems, etc.);
- *Metrics of Hosts* (Criticality Level, etc.);
- *Metrics of Attack Actions* (Damage Level; Access Complexity; Base Score; Confidentiality Impact; Availability Impact; Access Complexity, etc.);
- *Metrics of Attack Routes* (Route Length in Vulnerable Hosts; Route Average Base Score; Maximum Access Complexity; Damage level of route; Maximum damage level of route, etc.);
- *Metrics of Threats* (Minimum and Maximum Quantity of Different Vulnerable Hosts used for Threat Realization; Quantity of Different Routes; Risk level of threat);

Use of Security Metrics:

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 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.

The above metrics will create a reference level model about monitoring and improvement to contribute to the definition of the security level for evaluation, validation and the optimization of the security necessities. It will also contribute to the enhancement of the existing security practices and to the integration of information security to its business processes values.

V. Comparative Study

In the Previous Section we have talked about probably the most imperative Key Management Techniques in Mobile adhoc systems. In Comparative study we are going to think about these Key Management methods endless supplies of the Features like Reliability, Security, Scalability and Robustness. The Comparative Survey is made relying on the outcomes that are investigations from different examination works and diaries. Table I demonstrates the Comparative Survey of Key Management conspires in Mobile adhoc Networks. Give us a chance to examine about the highlights of Key Management plots that we are going to analyze.

Unwavering quality: The Reliability of a Key Management plan relies on the Key Distribution, Storage and Maintenance. It is important to verify that the Keys are Properly Distributed among the hubs, securely put away where interlopers aren't ready to hack the keys and ought to be Properly Maintained.

Versatility: Key administration operations ought to complete in an opportune way in spite of a fluctuating number of hubs and hub densities. The division of the accessible data transfer capacity involved by system administration activity ought to be kept as low as could reasonably be expected. Any increment in administration activity decreases accessible transmission capacity for payload information in like manner. Consequently, versatility of key-administration conventions is critical.

Security: Authentication and interruption resilience is an essential concern to guarantee no unapproved hub gets key material that can later be utilized to demonstrate status as a genuine individual from the system. No one ought to give private keys or issue authentications for others unless the others have been verified. Interruption resistance implies framework security ought not succumb to a solitary, or a couple of, traded off hubs. Other focal security issues are trust administration and powerlessness. Trust relations may change amid system lifetime. The framework ought to empower avoidance of traded off hubs. So as to judge the security of a key-administration plan, conceivable vulnerabilities ought to be pinpointed. Fitting key lengths and cryptographic calculations of satisfactory quality are expected.

Strength: The key-administration framework ought to make due regardless of foreswearing off administration assaults and occupied hubs. The key-administration operations ought to have the capacity to be finished regardless of broken hubs and hubs showing byzantine conduct, that is, hubs that deliberately go amiss from the convention. Important key administration operations created by element gathering changes ought to execute in an auspicious way. Key administration operations ought not oblige organize wide and strict synchronization.

International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 1, April 2015

Comparative Survey of the methods

TABLE I. Comparative Survey of the methods

	<i>Security</i>	<i>Scalability</i>	<i>Robustness</i>	<i>Reliability</i>
DKPS	Medium	Fair	Fair	Good
PIKE	Medium	Limited	Fair	Fair
INF	Low	Poor	Good	Good
SOKM	Medium	Fair	Fair	Good
SEKM	High	Good	Fair	Good
Private ID based Key	High	Good	Good	Fair
SEGK	Low	Poor	Good	Good
PGSK	High	Good	Fair	Good
Cluster based Key	Medium	Limited	Fair	Limited
Zone based Key	Low	Limited	Poor	Fair

In my research we focus on quantitative study of network security to reduce the vulnerability. So here we are showing the percentage of vulnerability.

Percentage of vulnerability, Security, Stability

TABLE II. Percentage of vulnerability, security, stability

<i>System</i>	<i>Vulnerability Assessment</i>	<i>Security Assessment</i>	<i>Stability Assessment</i>
CVSS	4.1%	3.9%	7.1%
CNSSA	5.21%	4.67%	7.68%
NSSA	6.71%	5.13%	7.99%

6.3 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

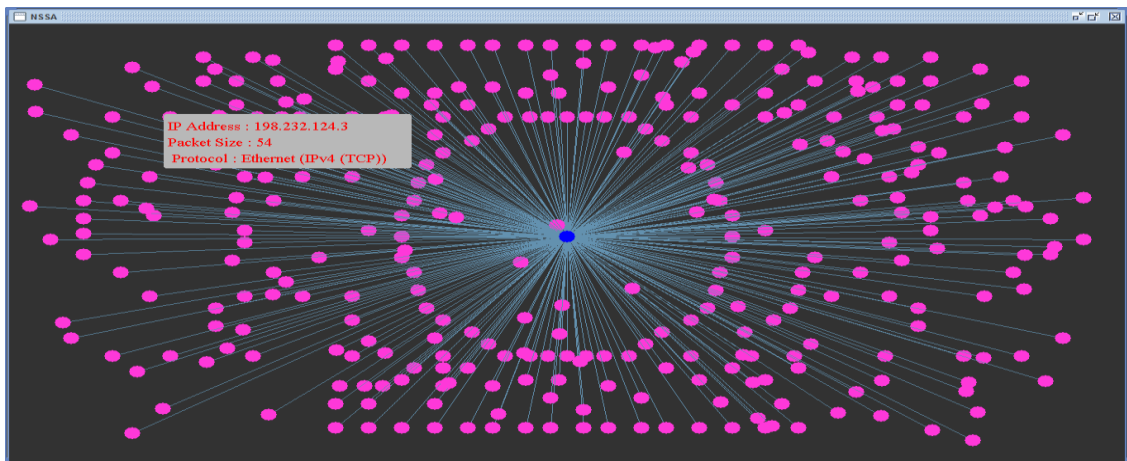


Fig. 4. Node detail graph

6.4 Showing Node detail Saved:

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

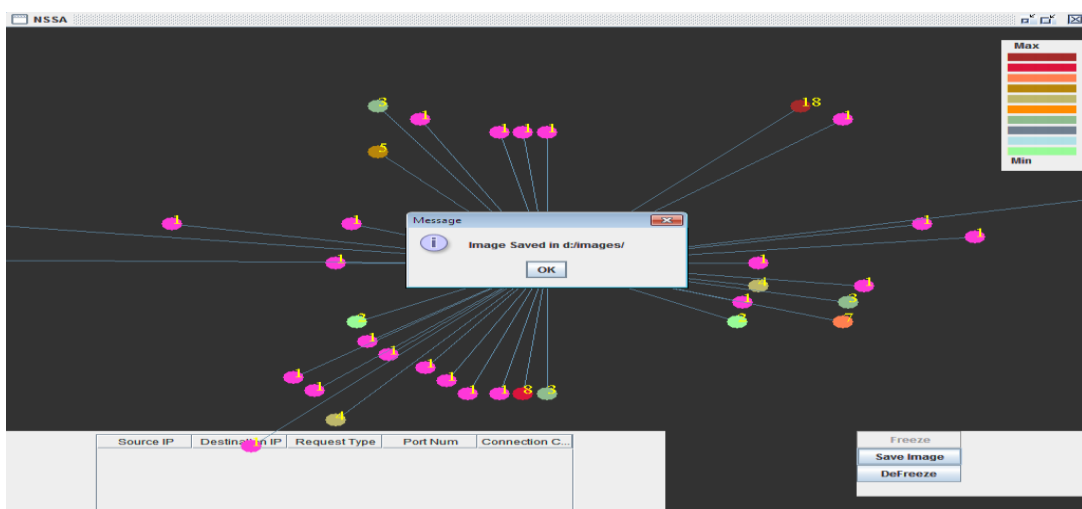
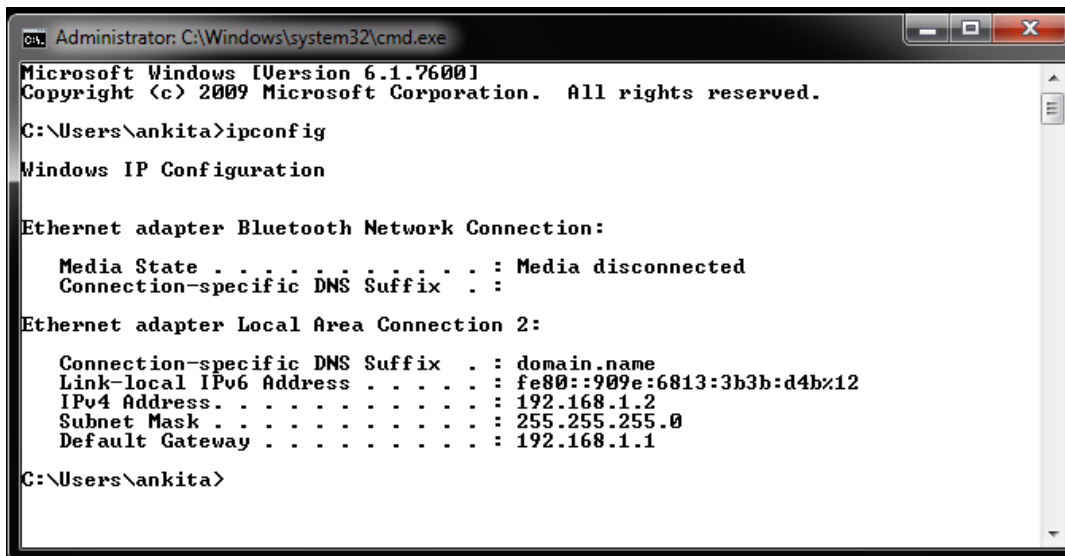


Fig. 5. Saved node detail

6.5 Detecting Attack:

This window show, when we type ipconfig it will show the source ip of the node.



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\ankita>ipconfig

Windows IP Configuration

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . :

Ethernet adapter Local Area Connection 2:

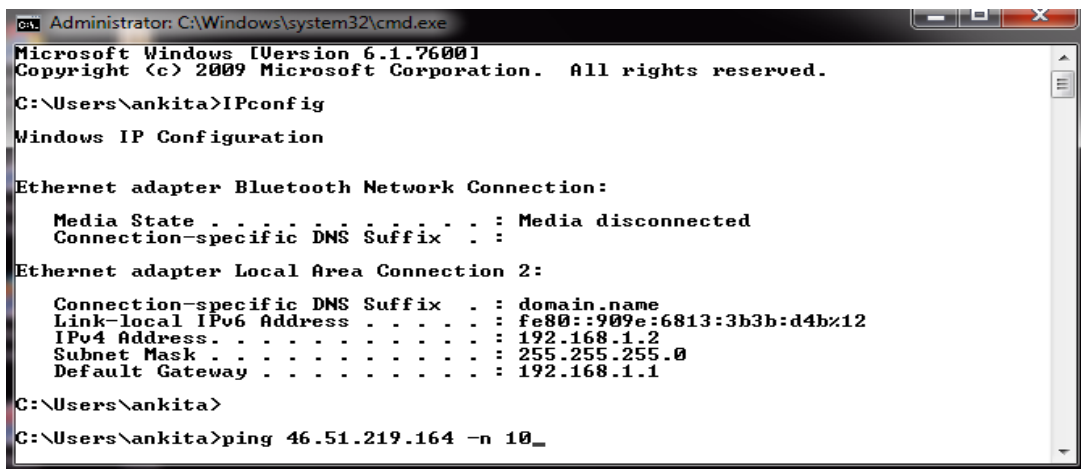
    Connection-specific DNS Suffix . . : domain.name
    Link-local IPv6 Address . . . . . : fe80::909e:6813:3b3b:d4b%12
    IPv4 Address. . . . . : 192.168.1.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\Users\ankita>
```

Fig.6. Detecting Attack

6.6 Showing attack:

When we run Ping command on command prompt it will detect which node having the maximum probability of attack.



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\ankita>IPconfig

Windows IP Configuration

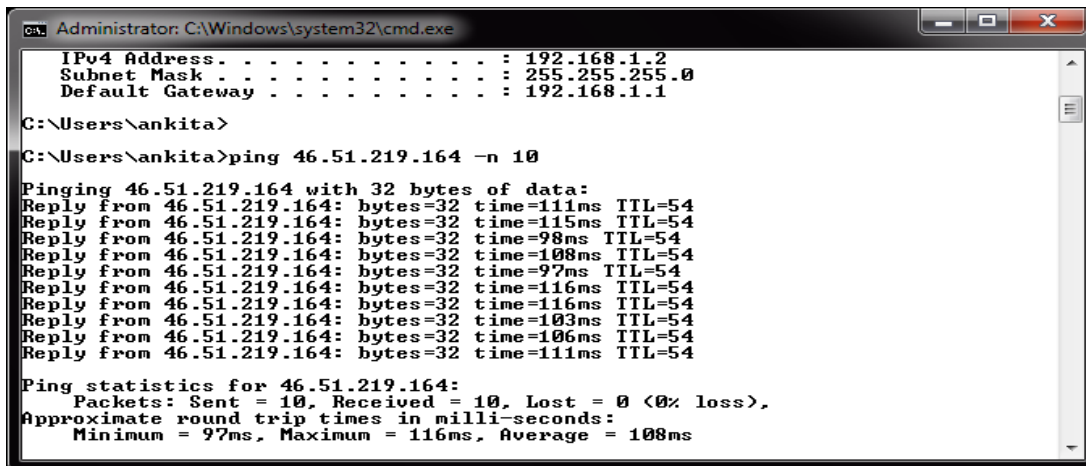
Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . :

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix . . : domain.name
    Link-local IPv6 Address . . . . . : fe80::909e:6813:3b3b:d4b%12
    IPv4 Address. . . . . : 192.168.1.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

C:\Users\ankita>
C:\Users\ankita>ping 46.51.219.164 -n 10_
```



```

Administrator: C:\Windows\system32\cmd.exe
IPv4 Address . . . . . : 192.168.1.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

C:\Users\ankita>
C:\Users\ankita>ping 46.51.219.164 -n 10

Pinging 46.51.219.164 with 32 bytes of data:
Reply from 46.51.219.164: bytes=32 time=111ms TTL=54
Reply from 46.51.219.164: bytes=32 time=115ms TTL=54
Reply from 46.51.219.164: bytes=32 time=98ms TTL=54
Reply from 46.51.219.164: bytes=32 time=108ms TTL=54
Reply from 46.51.219.164: bytes=32 time=97ms TTL=54
Reply from 46.51.219.164: bytes=32 time=116ms TTL=54
Reply from 46.51.219.164: bytes=32 time=116ms TTL=54
Reply from 46.51.219.164: bytes=32 time=103ms TTL=54
Reply from 46.51.219.164: bytes=32 time=106ms TTL=54
Reply from 46.51.219.164: bytes=32 time=111ms TTL=54

Ping statistics for 46.51.219.164:
    Packets: Sent = 10, Received = 10, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 97ms, Maximum = 116ms, Average = 108ms
  
```

Fig.7. Showing attack

VII. Conclusion

- Our approach gives way to an iterative visual investigation and enables recover discovery for more sophisticated attack patterns and anomalous features which are otherwise undetectable by standard network traffic visualization tools.
- The unique feature of the proposed system is real time analysis and behaviour plotting through attack graphs. It can also process different types of information simultaneously.
- At the initial level of research it proves as a better option for network and security administrator. Future results and implementation prototype will definitely makes the way open for various researchers.
- In visualizing a set of simple graph patterns, analysts can put together visual pieces of information conveyed by these smaller patterns and can learn about larger and more complex patterns.
- In this paper I have gave the comparative study of survey method according to their reliability, security, robustness, scalability and also shows the efficiency.

VIII. Future Work

System can further be extended to implement HRCAL scheme in real-time networks where it has to deal with the unwanted attacks. It is judged by the approach which can be added to exact, timely analysis based on graph generation which can solve the problem easily.

ACKNOWLEDGMENT

This research work is self financed but recommended from the institute so as to improve the security situations and breaches with current techniques. Thus, the authors thank the anonymous reviewers for their valuable comments, which strengthened the paper. The authors also wish to acknowledge SVITS administration for their support & motivation

International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 1, April 2015

during this research. They also like to give thanks to Mr. Vijay Prakash & Dr. Rajeev Vishwakarma for discussion regarding the situational awareness system & for producing the approach adapted for this paper.

REFERENCES

- [1] [1] 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.
- [2] 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.
- [3] Bon K. Sy, “Integrating intrusion alert information to aid forensic explanation: An analytical intrusion detection framework for distributive IDS”, in Elsevier Journal of Information Fusion, ISSN: 1566-2535, doi:10.1016/j.inffus.2009.01.001, 2009.
- [4] Igor Kotenko and Mikhail Stepashkin, “Attack Graph Based Evaluation of Network Security”, in International Federation for Information Processing, in LNCS 4237, 2006. Pp:216-227.
- [5] 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.
- [6] Wang, C. Yao, A. Singhal and S. Jajodia, “Network Security Analysis Using Attack Graphs :Interactive Analysis of Attack Graphs using Relational Queries”, in proceedings of IFIP WG Working Conference on Data and Application Security (DBSEC), 11.3 pages 119-132, 2006.
- [7] Attack Graph Based Evaluation of Network Security Igor Kotenko and Mikhail Stepashkin SPIIRAS, 39, 14 Liniya, St.-Petersburg, 199178, Russia.
- [8] Haines JW, Lippmann RP, Fried OJ, Tran E, Boswell S, Zissman MA. DARPA intrusion detection system evaluation: Design and procedures. Technical Report 1062, Lexington: MIT Lincoln Laboratory, 1999.
- [9] Lang F, Wang C, Gouqing M. " A Framework for network security situation awareness based on knowledge discovery" 2010 2nd International conference on computer Engineering and Technology.

**International Journal Of Core Engineering & Management (IJCEM)
Volume 2, Issue 1, April 2015**

- [10] Schiffman, M.: ‘A complete guide to the common vulnerability scoring system’, 2005. Available at: <http://www.first.org/cvss/cvss-guide.html>, accessed 9 March 2006.
- [11] 2 Forum of Incident Response and Security Teams (FIRST). FIRST web site, 2006. Available at: <http://www.first.org/>, accessed 9 March 2006.
- [12] Ankita Patil, Vijay Prakash “A Novel Framework for Network Security Situation Assessment Using HRCAL Approach” International journals of Engineering Science Research and Technology. May 2014.
- [13] Ankita Patil, Vijay Prakash “Performance Evaluation of Composite Network Security Situation Assessment Using HRCAL” International journals of Research in Computer Engineering and Electronics. Nov- Dec 26, 2014.
- [14] Ankita Patil, Vijay Prakash “Uniform Comparison Approach for Different Network security Assessment Using HRCAL Method” COMPUSOFT, An international journal of advanced computer technology, 4 (1), January-2014.