ISSN (Online): 2456-5717

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.1 Issue.5 August 2015

Anonymous Vulnerability Identification and Avoidance in Initiative IP Network

M. Masthan[1], R. Ravi[2]
[1]Research Scholar, Dept. of Computer Science and Engineering, Manonmaniam Sundaranar University, Tirunelveli, India.
[2]Professor and Head, Dept. of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli, India.

Abstract – **Network security is an essential factor for the Initiative IP Systems. The usage of collaborative IP networks has become more popular in this decade. Therefore cyber-attacks in networks will significantly reduce the reliability among the clients. In order to provide an efficient security to the network system, it is important to measure the security essentials of the network. So we can measure the amount of security solutions provided to a network by a network security metric. The contribution of this research work is all about, a novel methodology for anonymous vulnerability identification and avoidance in the Initiative IP Networks. This protocol will safeguards every session from different types of attacks. In addition to that, this protocol will monitor the database requests and avoid the attack earlier. The proposed framework also analyses the database for malware traces, to implement worms and virus detection. With the help of Topological Vulnerability Analysis (TVA) tool, analysis has been taken in which our proposed concept scoring to the vulnerabilities.**

Index Terms:- IP Security, Zero day vulnerability, identification, avoidance.

I. INTRODUCTION

Digital surveillance on big business are politically or socially predominant through the internet. The attackers targets the material and corporate association and are brought out through the spreading of virus dispersal, unauthorized web usage and the counterfeit site that taking information. The internet has turned out to be generally intricate, leaving numerous defenseless malicious attacks. Several organizations which are confronted to ensure their foundation against security attacks. Consistently, the security breaks cost organizations many dollars in income and gained notorieties. Initiative networks have turned out to be a crucial part to the organizations and administrative offices. As they keep on growing both in size and intricacy, the network security has turned into a basic concern. An initiative security objective is to diminish all systems and host vulnerabilities. Indeed, even a reasonably measured system can have a wide range of attacks, an attackers could increase their activity on any unauthorized system.

These organizations are facing so many affecting factors like increasing vulnerabilities, malicious attacks and information leakage etc. Some of the important attacks that the system could often experience are eavesdropping, man-in-middle attack, IP spoofing, denial of service, distributed denial of service etc. There has been developed retrievable tool technique protocols to prevent the cyber-attack, which can withstand the critical security threats in the recent organizational networks.

The major drawback of the computer network security is that the lacking of measure of the system security solution. So many indirect measurements such as firewalls are obtained; but they provide very little about the effectiveness of the security solutions when it is deployed in a real-world network. In such a case, a network security metric is used because, it would provide direct measurement of the effectiveness of the security solutions. Existing efforts provide a security metric, k zero day safety that simply counts how many distinct zero day vulnerabilities are required to compromise a network asset. A large count will provide more secure network. It requires tight time synchronization to detect the attacks and known geographic information to identify attacks and protect the network. It is not capable to detect attacks against routing such as worm hole, sink-hole attack and Sybil attacks. The attacker can easily create traffic collision with seemingly valid transmission drop or misdirect messages in routes.

To eradicate these problems, a novel zero day vulnerability protocol has designed in this paper. This protocol will not measure the amount of vulnerabilities to compromise a system, instead it provides several algorithms which were used to detect and prevent the vulnerabilities in the organizational network. Also this method provides an algorithm to detect the worm and virus in the organizational network. Using some of the known data about the security threats to the system, the suggested technique also having some score on the vulnerabilities. At last, we are using the CAULDRON analysis tool to analyze several other existing security mechanisms with the proposed methods.

II. RELATED WORKS

Poolsapasit N [3] describes an efficient algorithm which emphases the risk management methods focusing the Bayesian networks to manage the security of the networks. This may be the most reliable and scalable representations. In recent times, B. Bhargavain [5] observes that different security metrics will provide only a partial view of security and the authors then propose a framework for grouping the metrics attack graph and decision metric based on their relative importance. Attack graph for large networks can get complex and maintains an attribute template for the graph. The size of the attribute instance can be as large as the number of machines. The combination of similar type of security metric will generate more number of graphs. The research on network security metrics has attracted much attention. In another early work, M. Monga andS. Sicari [6] proposes a Cooke's classical method that will find previously unknown vulnerability in the software. An attack tree marked with abstract exploitability and hazard is passed to find sequences of attacks that corresponds to the easiest paths followed by potential attackers, and the amount of minimum effort needed along such paths is used as a security metric.

In another similar work C. Phillips and L. Swiller [11] proposes a graph based approach that analyses network vulnerability. It requires an input database of common attacks, specific network configuration and attacker profile. The length of shortest attack paths in terms of the number of exploits, conditions or both is taken as security metric for measuring the amount of security of networks. The main limitation of those early work lies in that they generally do not consider the relative security or likelihood of vulnerabilities.

In a network the important factor that focuses merely on the security metric and known vulnerabilities in the network. In paper [3] Holm and Sommestad designed an algorithm which shows the importance of the possible dependencies of vulnerabilities using a vulnerability enslavement chart. The damage values and the other threats cannot be explained easier than this method. Chaffin.M and Boyer [12] made a better research on the sum of all the zero day vulnerabilities depending on the datasets about the vulnerabilities analyzed in a single day. A derivation of logical ratio and Boolean variable that identifies every vulnerability proposed by Wang and jajodian [8].

III. PROPOSED METHOD

This protocol identifies and avoids the zero day vulnerability in the organizational IP networks. Numerous algorithms and protocols has been used by this proposed method to attain the objective of the reliable network. Initially this mechanism finds the overall possible routing paths followed by the most cost effective shortest path by employing the zero day shortest path algorithm. Thereafter by using a trust aware detection technique, the vulnerabilities in the networks are identified. The proposed approach also implements worm and virus detection to evaluate malware from data.

a) Zero day shortest path algorithm

This protocol uses a direct graph to determine the shortest path among the network from the sink node to the expected destination. Also the graph for the spanning tree will also be identified in this protocol. Finding the shortest path in a network is a commonly experienced problem. For example you want to reach a target in the real world via the shortest path or in a computer network a network package should be efficiently routed through the network. A network can be modeled by a graph. Routers are represented by nodes. Physical links between routers are represented by edges. Attached computers are used. Each edge is assigned a weight representing the overall time that the request process and response given to the client. The total cost of a path is the sum of the weights of the edges. The problem is to find the least-weight path. At the first iteration, the algorithm finds the closest node from the source node which must be a neighbour of the source node. At the second iteration, the algorithm finds the second-closest node from the source node. This node must be a neighbour of either the source node or the closest node found in the first iteration. At the third iteration, the algorithm finds the third-closest node from the source node. Either one of the initial two closest node or the source node must be neighbors. This algorithm identifies the kth node from the source node at the K^{th} iteration.

Pseudocode: Zero day_shortest

```
Input: Source, assets
Output: Assets with a non negative real number
Method:
Let wt[source] := 0
for each node v in G
    if v ≠ source
        wt[v] := infinity
    previous[v] := undefined
    Add v to Q
end for
while Q is not empty
    u := node in Q with min wt[u]
    remove u from Q
    for each neighbor v of u
        alt := wt[u] + leng(u, v)
        if alt<wt[v]
            wt[v] := alt
            previous[v] := u
return wt[], previous[]
```

b) Zero day Frame work Encryption Algorithm

This Zero day framework uses the Advanced Encryption Standard mechanism to avoid the zero day vulnerability. Symmetric block cipher is the building block of the AES. Framework use this for verifying whether the request comes from the valid client or not. The valid server connection is only possible through the abstract request. The request would be encrypted using one key and decrypted by the framework using the same key.

c) Trust Aware Detection Technique

Detection and avoidance of malicious threats to the network is the important objective of this Trust aware detection algorithm. This mechanism proves that, it is the most efficient technique to identify and avoid the harmful attacks. This technique can be implemented by the framework with low overhead. This technique can be integrated into existing routing protocols with the least effort, thus producing secure and efficient fully-functional protocols. It significantly reduce negative impacts from these attackers. It is also energy-efficient with acceptable overhead. It incorporates the trustworthiness of nodes into routing decisions and allows a node to circumvent an adversary misdirecting considerable traffic with a forged identity attained through replaying. It identifies such intruders that misdirect noticeable network traffic by their low trustworthiness and routes data through paths circumventing those intruders to achieve satisfactory throughput. is also energy-efficient, highly scalable, and well adaptable. The above technique enables a node to keep track of the trustworthiness of its neighbors and thus to select a reliable route and put in the routing table. The Trust Aware Detection Technique efficiently attains the energy conservation, eventhough the identification of malicious nodes misdirecting the packets.

d) Zero day Worm and Virus Detection Algorithm

The most important malicious threat to the organizational network is the security threat. These worm can be actively whitewashed by the antivirus tools. This tool uses pattern based identification to detect the worms. However the high spreading speed of worm results in anti-virus is less effective in detecting worms. Moreover, anti-virus cannot detect unknown internet worm automatically because it uses signature in detecting worms. Anti-virus compares the file structure of the worms with the signatures stored in its database. If they are matched, then the file is considered as infected by the worm. This required the anti-virus database to be frequently updated, so that it can detect new worms. This is the main reason what-virus cannot detect most of unknown internet worm automatically. Beside antivirus, firewalls and routers can be used to detect worm. Signature and block the worm, but this occurs only after the worm already spread. The worm generates an IP address and uses that IP address to communicate to potential victim, when the IP address is unused. The proposed Worm and Virus Detection Algorithm is used to detect the malwares from the data. This algorithm used for the file that have a huge size. It performs searching based on the three attributes, file type, file size and file content. It will check the worms in the file at random locations. It is the major advantage of getting the worms from the content. The number of comparisons are performed any number of times in the specified algorithm. This will be more applicable to the user to detect the malware from the content very accurately. The detection method which decides the rounds. An integer value will be returned if there is any match found. This may be able to specify the file is affected by virus or not. The proposed algorithm is efficient, time saving and less complex.

Pseudocode: Zero day_Worm and virus Detection

```
Input:File to Check
Output:An integer Value
Method:
Let M be the length of input file
Let N be the length of original File
for i=0 to N-M
    for j=0 to M
        if org[i+j] != inp[j]
            Return 0
        Else
            if j=M
                Return i
```

e) Common Vulnerability Scoring System (CVSS)

An open standard method for rating the IT vulnerabilities is the CVSS protocol. The environmental score can be calculated by using the temporal score and the temporal score can be analyzed by using the base score. Base represents the intrinsic and fundamental characteristics of vulnerability that are constant over time and user environments. Temporal represents the characteristics of vulnerability that change over time but not among user environments. Regarding the significant clients environment the characteristics of the vulnerabilities are identified.

f) Vulnerability Analysis using CAULDRON

In this section we are analyzing the existing protocols with the proposed method. The security metric will lags behind the necessary benchmark data. One viable approach would be integrated with the proposed model as an added feature to existing vulnerability analysis tool, such as CAULDRON to evaluate its practical effectiveness and to fine-tune the model. Cyber security is a global issue of growing importance. Cyber Espionage can affect technical, military, Political and economic interests anywhere. To protect critical networks, management must understand not only individual system vulnerabilities but also their interdependencies. Proposed System security analysis done by Topological Vulnerability tool that supports both offensive and defensive Applications. CAULDRON places Vulnerabilities and their protective measures within context of overall network security by modeling their interdependencies via attack graphs.

IV. SYSTEM ARCHITECTURE

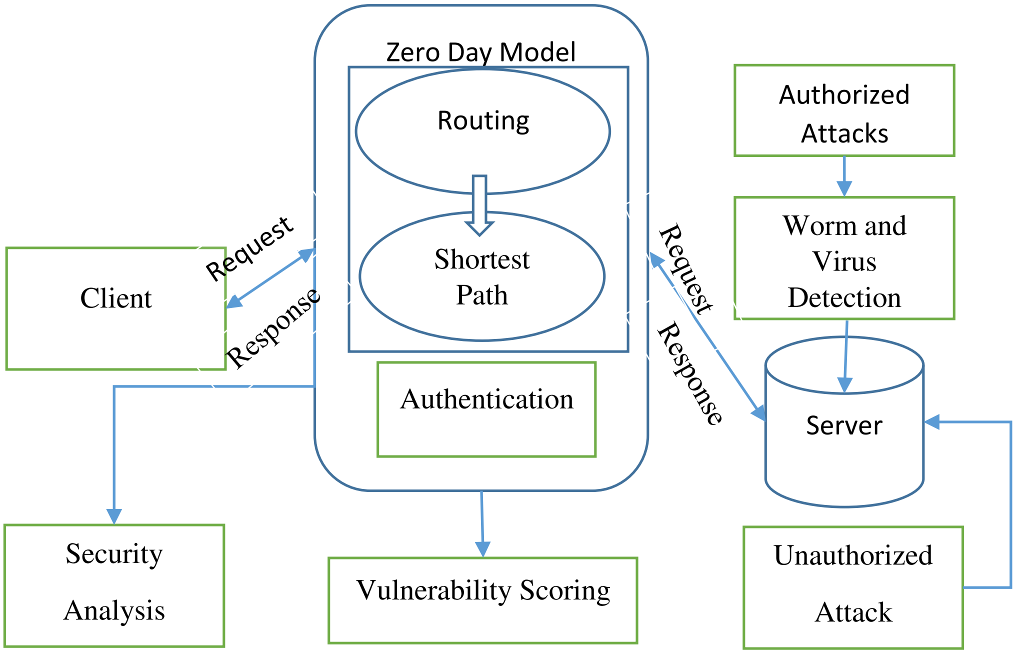


Fig.1 System Architecture

Figure 1 demonstrates the system design. Client gives request to the server. A valid server connection is only possible through the session value. The session value is encrypted and decrypted for authentication. It will provide more security. The system defines a zero Day Vulnerability Prevention Framework that detects and prevent and vulnerabilities on Enterprise IP network. This will identify the entire possible path that client connects to the destination and put it in the routing table. From the routing table it will find the shortest path based on the weights calculate on each node. Then it provides peer connection to the appropriate sever. Thus framework detects both authorized& unauthorized attacks. Unauthorized attack includes the client trying to connect without session or with different session. In such cases, the framework that prevents the attack by blocking particular IP and put it in a blacklist. The authorized attack will include the SQL Injection attack and prevention, File uploading attack. These attacks are detected and prevented by using Trust Aware Detection Techniques. This system mainly concentrated on the worm and virus detection by Naive Pattern Searching Algorithm. It will detect the malware from the data.

a) *Route Filtering and Path Identification*

The weight of each node will be calculated by the zero day vulnerability identification protocol. The validity of the client is further evaluated. The valid server connection is possible through the abstract session value. It then find the entire possible paths that client connects to the server. The entire possible path will be placed in the routing table. From the specified paths in the routing table, it will identify the shortest path based on the weight assigned in each node. It is the overall time that the request process and response given to the client.

b) *Authentication and Unauthorized Attack*

The proposed framework verifies each client whether authenticated or not. A valid server connection is only possible through the abstract session value. This session value is appended with the request to the server. Abstract session is a status value that will be encrypted. At the destination server it will be decrypted by the framework and connects to the server. This abstract session provides more security to the server connection. There will be a chance of unauthorized attack. It may be in the form request without abstract value and request having different abstract values or invalid abstract. The framework detects the unauthorized attacks based on trustaware detection technique by blocking the client from future access and put that into the blacklist.

c) *Route Filtering and Path Identification*

Initially the weight of each node will be calculated In the zero day vulnerability identification protocol. The validity of the client is ensured in this step. The valid server connection is possible through the abstract session value. It then find the entire possible paths that client connects to the server. The entire possible path will be placed in the routing table. The selection of shortest path is carried out, from the routing table depending upon the weight assigned to each node. The patch selection is the important factor, which determines the processing time for the request and response message to be received.

d) Authentication and Unauthorized Attack

The proposed framework verifies each client whether authenticated or not. A valid server connection is only possible through the abstract session value. This session value is appended with the request to the server. Abstract session is a status value that will be encrypted. At the destination server it will be decrypted by the framework and connects to the server. This abstract session provides more security to the server connection. There will be a chance of unauthorized attack. It may be in the form request without abstract value and request having different abstract values or invalid abstract. The framework detects the unauthorized attacks based on trust aware detection technique by blocking the client from future access and put that into the blacklist.

e) Authorized Attack Detection and Prevention

The biggest threats are security attacks from people within the organization. While external attacks are extremely important and critical, internal attacks should not be overlooked. The zero day vulnerability prevention framework thus detects an authorized attack also. They may include activities like SQL injection attacks, file uploading attacks. It is possible for attackers to provide a username containing SQL met characters that subvert the intended function of the SQL statements. When a client wants to get the details, that when it connects to the server, weight and all details these types of attacks occur. Consider the case admin`or`1`=`1. This allows an attacker to log in to the data, since OR expression is always true. Using the same technique attackers can inject other SQL commands which could extract modify or delete data within the database. Trust aware detection technique that detects such kinds of attacks and prevents by using prepared statements that helps in defending against SQL injection and move the IP to blacklist. File uploading attacks occurred during uploading files. The attacker uploads the files that virus affected. It will go for the Google search and collects all the files that are suspected to virus with same name. It will extend the database error files by adding the new searched Google items. Trust aware detection technique that detects the attacks and prevents based on the file name and blocks that IP.

f) Worm and Virus Detection

It evaluates malware from the content. Worms and viruses are self-replicating programs. It uses network to send copies of itself to other systems invisibly without user authorization. Zero day pattern search algorithm is used to find worm and virus based on the file type, size and content. Three parameters are used for evaluating the malwares from the content. It compares the size of the file and type of the file. Then it compares the content randomly at different location. The comparison round is determined by the authenticated person. If it detects any mismatch, it will detect the file is un trusted file. If there is no change in three parameters, it will be trusted file. The un trusted file will be moved to the database black list.

g) Vulnerability Scoring

Based on the severity the suggested protocol provides the scores for the vulnerability. The zero day vulnerability prevention framework that assigns scores to the vulnerabilities by integrating it with common venerability scoring system. It identifies and assesses vulnerabilities across many disparate hardware and software platforms. They need to prioritize these vulnerabilities and remediate those that pose the greatest risk. CVSS is composed of three metric groups: Base, Temporal, and Environmental, each consisting of a set of metrics. Base represents the intrinsic and fundamental characteristics of vulnerability that are constant over time and user environments. Temporal represents the characteristics of vulnerability that change over time but not among user environments. Environmental represents the characteristics of vulnerability that are relevant and unique to a particular user's environment. The purpose of the CVSS base group is to define and communicate the fundamental characteristics of vulnerability.

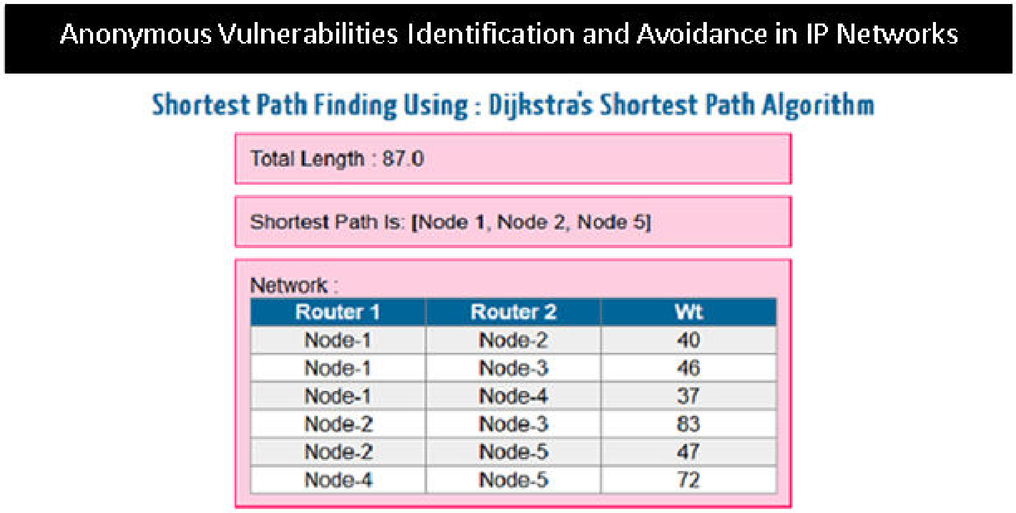
h) Security Analysis

The real time situational will be created by the integration and interchanging of the unprocessed security data by the CAULDRON tool. This mechanism analysis the vulnerability dependencies and provides attack information to the network. It accounts for sophisticated attack strategies that may penetrate an organization's layered defenses. CAULDRON's intelligent analysis engine reasons through attack dependencies, producing a map of all vulnerability paths that are then organized as an attack graph that conveys the impact of combined vulnerabilities on overall security. To manage attack graph complexity, CAULDRON includes hierarchical graph visualizations with high-level overviews and detail drill down, allowing users to navigate into a selected part of the big picture to get more information. They recently installed CAULDRON in their Cyber Security Incident Response Center and it is helping them prioritize security problems, reveal unseen attack paths and protect across large numbers of attack paths. While currently being used by the FAA and defense community, the software is applicable in almost any industry or organization with a network and resources they want to keep protected, such as banking or education. Because of vulnerability interdependencies across networks, a topological attack graph approach is needed for defense against multi-step attacks. The traditional approach that treats network data and events in isolation without the context provided by attack graphs is clearly insufficient. TVA combines vulnerabilities in ways that real attackers might do, discovering all attack paths through a network. Network Capture builds a model of the network, in terms of relevant security attributes. Vulnerability Database represents a comprehensive repository of reported vulnerabilities, with each vulnerability record listing the affected software.

IV. Discussions

The important goal of this suggested protocol is to identify and avoid the anonymous vulnerabilities in the organizational IP networks. This method implements an trust aware detection technique which avoids both the authorized and unauthorized attacks. This protocol is one of the best method in the identification and avoidance of attacks in the organizational IP networks. In large scale communication networks, this mechanism provides an efficient results. The application of this concepts is not limited to defense, communication management and large scale research purposes.

V. Simulation Results



Anonymous Vulnerabilities Identification and Avoidance in IP Networks

Shortest Path Finding Using : Dijkstra's Shortest Path Algorithm

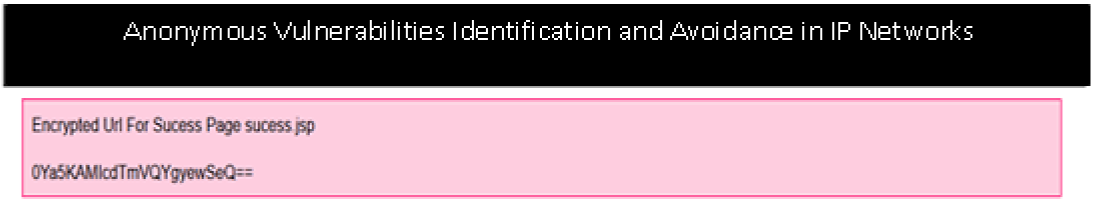
Total Length : 87.0

Shortest Path Is: [Node 1, Node 2, Node 5]

Network :

Router 1	Router 2	Wt
Node-1	Node-2	40
Node-1	Node-3	46
Node-1	Node-4	37
Node-2	Node-3	83
Node-2	Node-5	47
Node-4	Node-5	72

Fig. 2 Shortest path



Anonymous Vulnerabilities Identification and Avoidance in IP Networks

Encrypted Url For Sucess Page sucess.jsp

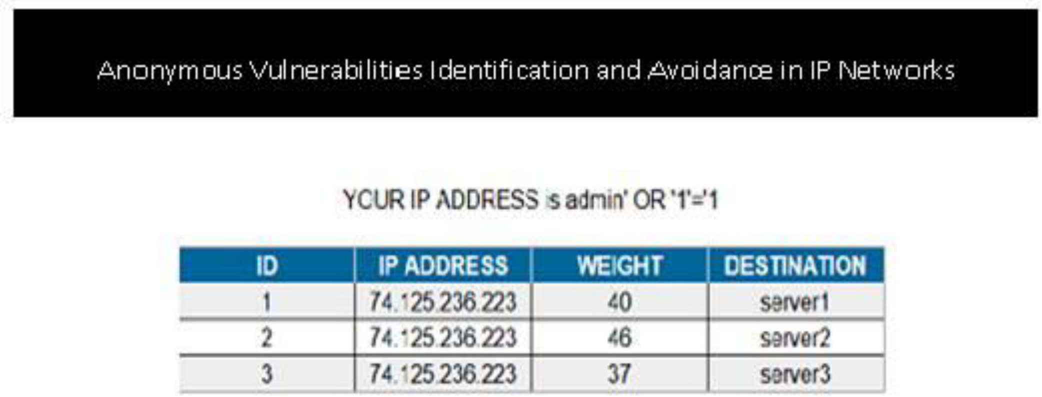
0Ya5KAMIcdTmVQYgyewSeQ==

Fig. 3 Abstract Request

Anonymous Vulnerabilities Identification and Avoidance in IP Networks

cdTmVQYgyewSeQ==

Fig. 4 File Decryption



Anonymous Vulnerabilities Identification and Avoidance in IP Networks

YOUR IP ADDRESS is admin' OR '1'='1

ID	IP ADDRESS	WEIGHT	DESTINATION
1	74.125.236.223	40	server1
2	74.125.236.223	46	server2
3	74.125.236.223	37	server3

Fig. 5 Authorized Attack

VI. CONCLUSION

A novel efficient zero day has vulnerability avoidance protocoled to identify and avoid the anonymous vulnerabilities in the network. Initially this protocol identifies whether the sensor node is active or dead. This protocol checks for the significant senor node that, it compromises with the malicious nodes or not. To ensure a secure and reliable communication between the sensor nodes, this protocol uses trust aware detection techniques. So that it can provide a reliable communication link during data transmission. At the time of data transmission, this protocol selects a trustable alternate route and blocking all other alternate paths. Secondly, the suggested approach measures the attackers and malware files from the dataset by the implementation of worm and virus detection protocol. At last, an analysis is carried out with the existing protocols that, the results were proving the fact that the suggested algorithm outperforms the available protocols. The tool used for the experimental analysis is the CAULDRON tool. The future research concepts in this area expands to the penetration testing in the zero day vulnerability identification and prevention protocols in the organizational IP Networks. Also to expand the ideas of attack detection by holding different types of attacks without providing the data connection.

REFERENCES

[1] H. Holm, M. Ekstedt, and D. Andersson, "Empirical Analysis of System-Level Vulnerability Metrics through Actual Attacks, "IEEE Trans. Dependable Secure Computing, vol. 9, no. 6, pp. 825-837, Nov. 2012.

[2] T. Sommestad, H. Holm, and M. Ekstedt, "Effort Estimates for Vulnerability Discovery Projects, " Proc. 45th Hawaii Int'l Conf. System Sciences (HICSS '12), pp. 5564-5573, 2012.

[3] N. Poolsappasit, R. Dewri, and I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs, " IEEE Trans. Dependable Secure Computing, vol. 9, no. 1, pp. 61-74, Jan. 2012.

[4] M. Shahzad, M. Shafiq, and A. Liu, "A Large Scale Exploratory Analysis of Software Vulnerability Life Cycles, " Proc. 34th Int'lConf. Software Eng. (ICSE '12), 2012.

[5] N. Idika and B. Bhargava, "Extending Attack GraphBased Security Metrics and Aggregating Their Application, " IEEE Trans. Dependable and Secure Computing, vol. 9, no. 1, pp. 75-85, Jan. /Feb. 2012.

[6] D. Balzarotti, M. Monga, and S. Sicari, "Assessing the Risk of Using Vulnerable Components, " Proc. ACM Second Workshop Quality of Protection (QoP '05), pp. 65-78, 2005.

[7] L. Wang, S. Noel, and S. Jajodia, "Minimum-Cost Network Hardening Using Attack Graphs, " Computer Comm., vol. 29, no. 18, pp. 3812-3824, 2006.

[8] J. W. P. Manadhata, "An Attack Surface Metric, " Technical Report CMU-CS-05-155, Carnegie Mellon University, 2005.

[9] S. Jajodia, S. Noel, and B. O'Berry, "Topological Analysis of Network Attack Vulnerability, " Managing Cyber Threats: Issues, Approaches and Challenges, V. Kumar, J. Srivastava, and A. Lazarevic, eds., Kluwer Academic, 2003.

[10] P. Ammann, D. Wijesekera, and S. Kaushik, "Scalable, Graph-Based Network Vulnerability Analysis, " Proc. Ninth ACM Conf. Computer Comm. Security (CCS '02), pp. 217-224, 2002.

[11] C. Phillips and L. Swiler, "A Graph-Based System for Network-Vulnerability Analysis, " Proc. New Security Paradigms Workshop (NSPW '98), 1998.

[12] M. McQueen, T. McQueen, W. Boyer, and M. Chaffin, "Empirical Estimates and Observations of 0Day Vulnerabilities, " Proc. Hawaii.