International Journal of Pure and Applied Mathematics
Volume 116 No. 10 2017, 21-25
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

A SURVEY ON NETWORK SECURITY TECHNIQUES

Mr. A.V.Allin geo[1], Mrs.K.Shanmugapriya[2]
[1,2]Assistant Professor, Dept. of CSE, BIST,BIHER,Bharath University, Chennai, Tamil Nadu
[1]sharveshvinay@gmail.com, [2]seemeallin@gmail.com

Abstract: The network security is an association technique and arrangements for guaranteeing the security of its advantages and of all system movement. At present, the system constitutes as a centre segment for data handling framework in different regions like money related area, influence eras and crisis frameworks. These frameworks are constantly utilizing distinctive sorts of data's from different areas. It is too difficult for network security engineers to be aware of the huge amount of data produced, at the same time it has been proved that depending on one tools is not enough to protect the network from being exploited. In 1999 Bass Tim was the first author who recommended the application of Situational Awareness in the future Network Security(NSSA).NSSA is a discipline which focuses on perception, evaluation, projection and resolution of the security risk to the computer networks.

Keywords: Vulnerability, Security, Stability, NSSA(NetworkSecuritySituationAwareness).

1. Introduction

The network security is an entangled subject. Arrange has been characterized as any arrangement of interlinking lines looking like a net, a system of streets an interconnected framework, a system partnerships. These frameworks are constantly utilizing diverse sorts of information's from numerous areas. In such circumstances where information is producing and getting refreshed frequently from different closures recognizing its conduct and legitimacy is a basic zone of work for specialists. Security of these systems from noxious interruptions is noteworthy to the economy and of our kin. Along these lines a standard approach to gauge organize security will unites distinctive clients with sellers and analysts. Over the most recent couple of years there has been some critical enhancements over giving institutionalizing such safety efforts utilizing: Topological Vulnerability Analysis, Network Hardening and Attack Response. To give the better security against the enormous assaults in the Internet, there is growing popularity for system examiners to think about the circumstances of system security successfully [1]. The current instrument needs such usefulness of investigating and speaking to the genuine system conduct. For each system and security, suppositions, the present concentrate is on subjective viewpoints instead of a quantitative investigation. Consequently, to gauge the general security of a system one should first comprehend the vulnerabilities and how they can be consolidated to build an assault which is hurtful for system. In this procedure it functions as a basic leadership strategy which has the expectation of assault weakness on a chose gadget. The gauge demonstrates that the assault example is completely coordinated by already keep qualities and its effect is investigated. in accordance with known learning the decision should be taken to educate alternate hubs, by Associate in ready message. Hence, by the on top of strategy it's deliberate scientifically that the assault defencelessness will be identified extra precisely continuously. Existing methodologies had circumstance mindfulness comprise of weakness investigation utilizing assault diagrams, interruption acknowledgment and ready affiliation, assault examination, assault affect investigation and criminology and data stream examination. Along these lines this work recognizes such limits from which assault safe framework can be isolated from real changes by mapping those parameters on representation system. It utilizes measurements based estimation for accomplishing its objective in convenient premise.

2. Related work

It directs an exceptional model SIEM (Security information and Event Management) for assault assessments. The advancement measures the conduct of existing assaults and in this manner the producing hubs for right investigation through a standard assault chart generator. It utilizes various security measurements for giving right hazard examination all through assault displaying security part (AMSEC) execution stage. The paper conjointly displays relate exemplification show for result analysis [1]. The paper [2], creator recommended a novel structure for security assessment with assault displaying utilizing SIEM (Security Information and Event Management) framework. It is completely in light of web information for better examination of security circumstances and current assault inclusions. The proposed administration framework depends on assault

investigation utilizing villain conduct distinguishing proof and chart era through different measurements for hazard appraisal. The paper likewise introduced a model for future execution in view of proposed approach. Basically it is figuring the powerlessness utilizing intelligent choices. Aside from the above powerlessness distinguishing proof instrument there are some component which is intended to recognize the intruder's procedure and their affections. One of that is AIDF (diagnostic interruption recognition structure) which is proposed in [3]. It utilizes a probabilistic deduction instrument for producing the most likely scientific elucidation in light of simply the useful interruption identification cautions, as well as the unreported mark decides that are uncovered in the likelihood display. It is frequently for IDs to be opened in full logging mode for the scientific information gathering. It can be considered as handy execution and arrangement of hostile to DOS methodology in a real world organization. Such a variety of creators had additionally dealt with decreasing the intricacy so such frameworks which are excessively perplexing, making it impossible to execute for a littler frameworks.

Issues of vulnerability analysis

The point is to identify the unusual designs or patterns and from this anticipate the future effects of the assaults on said gadgets. Subsequent to concentrate the different existing methodology in the distinctive regions of the system utilised for expectations and gauging, this work had distinguish that examiner need to know the designs in a confined way and the discovery is completely in view of sensible capacities of few of those. Therefore, some computerisation is required for better comprehension of vulnerabilities and impacts of assaults. Here are the some distinguished issues in existing methodologies for settling the issues of vulnerability investigation.

Issue 1: The entire current framework will consider powerlessness in a subjective angle instead of some quantitative viewpoints which delude the analyst's.

Issue 2: Real time estimation is not given by which misfortunes are nearly bigger than others.

Issue 3: Massive information handling some time produces false caution and inaccurate forecasts along these lines expectation exactness should be considered as essential parameters for the work.

Issue 4: The appraisal used to arrange organize state and the level of data required for ideal delineation is not finished dependably which mislead the forecast.

3. Proposed system

This workproposes a comparative study of the NSSA with other different network security aspects. The other different security networks are the CNSSA(a Comprehensive Network Security Situation Awareness) and the CSSV(Common Vulnerability Scoring System), with these two network securities we are going to compare the NSSA .The CNSSA is to perceive network security situations comprehensively. Based on the network information fusion, it makes a quantitative assessment on the network security situations. The CNSSA visualizes the situations of network security in its various and multiple views, so that the network analyst can know about the network security situations easily and comprehensively. The Common Vulnerability Scoring System (CVSS) is an open framework for communicating characteristics and severity of software vulnerabilities. CVS has three metrics: Base, Temporal and Environmental. A CVSS score can also be represented as vector string, a compressed textual representation of the values used to derive the score.

The bar-graph is also provided for this. There are a few advantages of utilizing the measurements in this work given here as:

1) Improved execution and insurance level of the framework.

2) Monitoring model which contrasts the present qualities and perfect values after which approval of operations and changes is measured.

3) Contribute to the improvement of the current security rehearses and to the incorporation of data security to its business forms values.

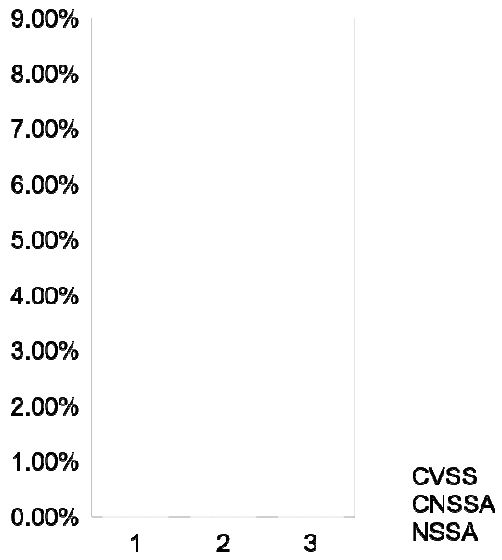
4. Comparative study

In this exploration we concentrate on quantitative investigation of system security to decrease the vulnerability. So here we are demonstrating the rate of vulnerability.

The Percentage of vulnerability, Security, Stability is

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

The graph representation for the above vulnerability table is, given below



5. Conclusion

Our approach offers path to an iterative visual examination and empowers recuperate disclosure for more complex assault designs and peculiar components which are generally imperceptible by standard system activity perception devices. The one of a kind component of the proposed framework is constant investigation and conduct plotting through assault diagrams. It can likewise prepare diverse sorts of data all the while. At the underlying level of research it demonstrates as a superior choice for system and security manager. Future outcomes and usage model will make the path open for different scientists. In envisioning an arrangement of straightforward chart designs, experts can assemble visual snippets of data passed on by these littler examples and can find out about bigger and more mind boggling designs. In this paper it has the relative investigation of overview strategy as per their dependability, security, heartiness, adaptability and furthermore demonstrates the proficiency.

References

[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]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.

[3]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.

[4]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.

[5]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.

[6]Attack Graph Based Evaluation of Network Security Igor Kotenko and Mikhail Stepashkin SPIIRAS, 39, 14 Liniya, St.-Petersburg, 199178, Russia.

[7]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.

[8]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.

[9]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.

[10]Forum of Incident Response and Security Teams (FIRST).FIRST web site, 2006. Available at: http://www.first.org/, accessed 9 March 2006.

[11] Udayakumar R., Kaliyamurthie K.P., Khanaa, Thooyamani K.P., Data mining a boon: Predictive system for university topper women in academia, World Applied Sciences Journal, v-29, i-14, pp-86-90, 2014.

[12] Kaliyamurthie K.P., Parameswari D., Udayakumar R., QOS aware privacy preserving location monitoring in wireless sensor network, Indian Journal of Science and Technology, v-6, i-SUPPL5, pp-4648-4652, 2013.

[13] BrinthaRajakumari S., Nalini C., An efficient cost model for data storage with horizontal layout in the cloud, Indian Journal of Science and Technology, v-7, i-, pp-45-46, 2014.

[14] BrinthaRajakumari S., Nalini C., An efficient data mining dataset preparation using aggregation in relational database, Indian Journal of Science and Technology, v-7, i-, pp-44-46, 2014.

[15] Khanna V., Mohanta K., Saravanan T., Recovery of link quality degradation in wireless mesh networks, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4837-4843, 2013.

[16]Khanaa V., Thooyamani K.P., Udayakumar R., A secure and efficient authentication system for distributed wireless sensor network, World Applied Sciences Journal, v-29, i-14, pp-304-308, 2014.

[17]Udayakumar R., Khanaa V., Saravanan T., Saritha G., Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction, Middle - East Journal of Scientific Research, v-16, i-12, pp-1781-1785, 2013.
[18]Khanaa V., Mohanta K., Saravanan. T., Performance analysis of FTTH using GEPON in direct and external modulation, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4848-4852, 2013.
[19]Kaliyamurthie K.P., Udayakumar R., Parameswari D., Mugunthan S.N., Highly secured online voting system over network, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4831-4836, 2013.
[20]Thooyamani K.P., Khanaa V., Udayakumar R., Efficiently measuring denial of service attacks using appropriate metrics, Middle - East Journal of Scientific Research, v-20, i-12, pp-2464-2470, 2014.
[21]R.Kalaiprasath, R.Elankavi, Dr.R.Udayakumar, Cloud Information Accountability (Cia) Framework Ensuring Accountability Of Data In Cloud And Security In End To End Process In Cloud Terminology, International Journal Of Civil Engineering And Technology (Ijciet)Volume 8, Issue 4, Pp. 376–385, April 2017.
[22]R.Elankavi, R.Kalaiprasath, Dr.R.Udayakumar, A fast clustering algorithm for high-dimensional data, International Journal Of Civil Engineering And Technology (Ijciet), Volume 8, Issue 5, Pp. 1220–1227, May 2017.
[23] R. Kalaiprasath, R. Elankavi and Dr. R. Udayakumar. Cloud. Security and Compliance - A Semantic Approach in End to End Security, International Journal Of Mechanical Engineering And Technology (Ijmet), Volume 8, Issue 5, pp-987-994, May 2017.
[24]Thooyamani K.P., Khanaa V., Udayakumar R., Virtual instrumentation based process of agriculture by automation, Middle - East Journal of Scientific Research, v-20, i-12, pp-2604-2612, 2014.
[25]Udayakumar R., Thooyamani K.P., Khanaa, Random projection based data perturbation using geometric transformation, World Applied Sciences Journal, v-29, i-14, pp-19-24, 2014.
[26] Udayakumar R., Thooyamani K.P., Khanaa, Deploying site-to-site VPN connectivity: MPLS Vs IPSec, World Applied Sciences Journal, v-29, i-14, pp-6-10, 2014.