Abstract

Today, there is a serious challenge facing Network Security, especially Networking Intrusion Detection and prevention attacks of Denial of Service. Denial of Service (DoS) has the most devastating effects on Networking and Information security. It has also put tremendous pressure over the security experts lately, in bringing out effective defense solutions. The adversary methods are ever changing day night, the complexity and sophistication of attacks and vulnerability methods continue to rise yearly, and the potential impact to the bottom line is significant organization information systems. These attacks could be implemented diversely with a variety of tools and techniques. Since there is no single solution for DoS, this attack has managed to prevail on internet for nearly a decade. The task of uncovering previous unseen DOS attacks and new attacks in dynamic Intranet networks quickly becomes unmanageable. Network Intrusion Detection Systems (NIDS) have become a necessity in information security model because of the increase DOS and malicious activities. Therefore, the research proposes a Data mining technique enhanced with Artificial intelligent that is classification, clustering, and Behavior profiling networks algorithm to categorize a network process as either normal or
Adaptive Network Intrusion Detection and Mitigation Model using Clustering and Bayesian Algorithm in a Dynamic Environment

abnormal. Prevention of DOS attacks using techniques as Quarantine IP address, Blackholing, Sinkholing. The proposed model Adaptive Network Intrusion Detection Model (ANIDM) based on the combination of techniques artificial intelligent and anomaly detection. Which is self-learning and adaptive in presence of DOS attacks and malicious activities under minimal human intervention. The proposed model is based on clustering and classification through K-NN algorithm. The results show that these mitigation approaches improve the ability to separate between unknown abnormalities in the dataset and the legitimate traffic structure. The ANIDM can effectively detects existing and new attacks focusing on Denial of service attack (DOS), while providing continuous service even under attacks. The model is based on speed, crypt-isolation, log-audit and preemptively restored on a regular basis. The model can be applied to Dynamic environment learning institution and business enterprise. Finding the primary challenges to Network intrusion detection are the problem of misjudgment, previous unseen attacks, overwhelming volume of false alarms, misdetection, new attacks tactics. Therefore, the paper concludes that variation ANIDM can be considered for detection and mitigate of DoS and DDOS attacks.

**References**

1. Verma, K., H. Hasbullah, and A. Kumar. An efficient defense method against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET. in 2013 3rd IEEE International Advance Computing Conference (IACC). 2013.
2. Singh, S., et al. Intrusion Detection Based On Artificial Intelligence Techniques. in International Conference Of Advance Research And Innovation (Icari-2014). 2014.
3. Xu, K., Z.-L. Zhang, and S. Bhattacharyya, Internet traffic behavior profiling for network security monitoring. IEEE/ACM Transactions On Networking, 2008. 16(6): p. 1241-1252.
4. Tan, Z., et al., Detection of Denial-of-Service Attacks Based on Computer Vision Techniques. IEEE Transactions on Computers, 2015. 64(9): p. 2519-2533.
5. Dadhich, A. and S.K. Yadav, Evolutionary Algorithms, Fuzzy Logic and Artificial Immune Systems applied to Cryptography and Cryptanalysis: State-of-the-art review. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2014. 3(6).
6. Chang, S. and T.E. Daniels. Correlation based node behavior profiling for enterprise network security. in 2009 Third International Conference on Emerging Security Information, Systems and Technologies. 2009. IEEE.
7. Sharma, S.K., et al. An improved network intrusion detection technique based on k-means clustering via Naïve bayes classification. in Advances in Engineering, Science and Management (ICAESM), 2012 International Conference on. 2012.
8. Xu, K., F. Wang, and L. Gu. Network-aware behavior clustering of Internet end hosts. in INFOCOM, 2011 Proceedings IEEE. 2011. IEEE.
9. Zhao, Y. Network intrusion detection system model based on data mining. in 2016 17th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD). 2016.
10. Yang, H., et al., A survey of artificial immune system based intrusion detection. The Scientific World Journal, 2014. 2014.
11. Murugan, S. and K. Kuppusamy. System and methodology for unknown Malware attack. in Sustainable Energy and Intelligent Systems (SEISCON 2011), International Conference on. 2011.
12. Midzić, A., Z. Avdagic, and S. Omanovic. Intrusion detection system modeling based on neural networks and fuzzy logic. in 2016 IEEE 20th Jubilee International Conference on Intelligent Engineering Systems (INES). 2016.

13. Kusumah, P., S. Sutikno, and Y. Rosmansyah. Model design of information security governance assessment with collaborative integration of COBIT 5 and ITIL (case study: INTRAC). in ICT For Smart Society (ICISS), 2014 International Conference on. 2014. IEEE.

14. Yan, Q. and F.R. Yu, Distributed denial of service attacks in software-defined networking with cloud computing. IEEE Communications Magazine, 2015. 53(4): p. 52-59.

15. Buczak, A.L. and E. Guven, A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials, 2016. 18(2): p. 1153-1176.

16. Sou, S.I. and C.S. Lin, Random Packet Inspection Scheme for Network Intrusion Prevention in LTE Core Networks. IEEE Transactions on Vehicular Technology, 2017. 66(9): p. 8385-8397.

17. Stampar, M. and K. Fertalj. Artificial intelligence in network intrusion detection. in Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015 38th International Convention on. 2015.

18. Goldstein, M., et al. Bayes Optimal DDoS Mitigation by Adaptive History-Based IP Filtering. in Seventh International Conference on Networking (ICN 2008). 2008.

19. Farid, D.M. and M.Z. Rahman, Anomaly Network Intrusion Detection Based on Improved Self Adaptive Bayesian Algorithm. JCP, 2010. 5(1): p. 23-31.

20. Degeler, V., R. French, and K. Jones. Self-Healing Intrusion Detection System Concept. in 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS). 2016.

21. Lorandel, J., J.C. Prévotet, and M. Héléard. Efficient modelling of FPGA-based IP blocks using neural networks. in 2016 International Symposium on Wireless Communication Systems (ISWCS). 2016.

22. Kwon, D., et al., A survey of deep learning-based network anomaly detection. Cluster Computing, 2017.

23. Frias-Martinez, V., et al. A network access control mechanism based on behavior profiles. in Computer Security Applications Conference, 2009. ACSAC’09. Annual. 2009. IEEE.

24. Kumar, M., M. Hanumanthappa, and T.V.S. Kumar. Intrusion Detection System using decision tree algorithm. in Communication Technology (ICCT), 2012 IEEE 14th International Conference on. 2012.

25. Reddy, R.R., Y. Ramadevi, and K.V.N. Sunitha. Enhanced anomaly detection using ensemble support vector machine. in 2017 International Conference on Big Data Analytics and Computational Intelligence (ICBDAC). 2017.

26. Gharaiibeh, M., et al. Assessing co-locality of IP blocks. in 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). 2016.

27. Schinagl, S., R. Paans, and K. Schoon. The Revival of Ancient Information Security Models, Insight in Risks and Selection of Measures. in 2016 49th Hawaii International Conference on System Sciences (HICSS). 2016. IEEE.

28. Jyothsna, V., V.R. Prasad, and K.M. Prasad, A review of anomaly based intrusion detection systems. International Journal of Computer Applications, 2011. 28(7): p. 26-35.

29. Sahu, S.K., S. Sarangi, and S.K. Jena. A detail analysis on intrusion detection datasets.
in Advance Computing Conference (IACC), 2014 IEEE International. 2014.

30. Chandrasekhar, A. and K. Raghuveer. Intrusion detection technique by using k-means, fuzzy neural network and SVM classifiers. in Computer Communication and Informatics (ICCCI), 2013 International Conference on. 2013. IEEE.

31. Cui, X., J. Beaver, and T. Potok. Swarm-Based Knowledge Discovery for Intrusion Behavior Discovering. in 2010 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. 2010.

32. Varuna, S. and P. Natesan. An integration of k-means clustering and naïve bayes classifier for Intrusion Detection. in Signal Processing, Communication and Networking (ICSCN), 2015 3rd International Conference on. 2015.

33. He, D., et al., Software-Defined-Networking-Enabled Traffic Anomaly Detection and Mitigation. IEEE Internet of Things Journal, 2017. PP(99): p. 1-1.

Index Terms

Computer Science Security

Keywords

Network Security Smurf, Neptune, Ping-Of-Death (POD), ICMP, Back, LAND (Local Area Network Denial & KDD Cup 99 Dataset, Dedicate to my family and all A.I, Datamining, Hackathons and knowledge discovery all of me for all of us.