{tag} {/tag}
IJCA Proceedings on EGovernance and Cloud Computing Services - 2012
by IJCA Journal

EGOV - Number 4

Year of Publication: 2012

Authors:
Meenakshi R M

E. Saravanan

{bibtex}egov1032.bib{/bibtex}

Abstract

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a Management Station. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPS for other purposes, such as identifying problems with security policies, documenting existing threats, and deterring individuals from violating security policies. IDPS have become a necessary addition to the security infrastructure of nearly every organization. False positives and false negatives happen

toevery intrusion detection and intrusion preventionsystem. This work proposes a mechanismfor false positive/negative assessment with multipleIDSs/IPSs to collect FP and FN cases fromreal-world traffic and statistically analyze thesecases. Over a period of 16 months, more than2000 FPs and FNs have been collected and analyzed. From the statistical analysis results, weobtain three interesting findings. First, morethan 92. 85 percent of false cases are FPs even ifthe numbers of attack types for FP and FN aresimilar. That is mainly because the behavior ofapplications or the format of the applicationcontent is self-defined; that is, there is not completeconformance to the specifications of RFCs. accordingly, when this application meets anIDS/IPS with strict detection rules, its traffic willbe regarded as malicious traffic, resulting in a lotof FPs. Second, about 91 percent of FP alerts,equal to about 85 percent of false cases, are notrelated to security issues, but to management policy. For example, some companies and campuseslimit or forbid their employees and studentsfrom using peer-to-peer applications; therefore,in order to easily detect P2P traffic, an IDS/IPSis configured to be sensitive to it. Hence, thiscauses alerts to be triggered easily regardless ofwhether the P2P application has malicious trafficor not. The last finding shows that buffer overflow,SQL server attacks, and worm slammerattacks account for 93 percent of FNs, eventhough they are aged attacks. This indicates thatthese attacks always have new variations toevade IDS/IPS detection.

References

- H. G. Kayac?k and A. N. Zincir-Heywood, "Using Intrusion Detection Systems with a Firewall: Evaluation on DARPA 99 Dataset", Project in Dalhousie University, [Online]. Available:http://projects. cs. dal. ca/projectx/files/NIMS06-2003. pdf.
- DARPA 99 Intrusion Detection Data Set Attack Documentation. [Online]. Available: http://www. ll. mit. edu/IST/ideval/docs/1999/attackDB. html.
- V. Corey, C. Peterman, S. Shearin, M. S. Greenberg, J. V. Bokkelen, "Network Forensics Analysis," IEEE Internet Computing, vol. 06, no. 6, pp. 60-66, 2002.
- W. D. Yu, D. Aravind, P. Supthaweesuk, "Software Vulnerability Analysis for Web Services Software Systems," iscc, pp. 740-748, 11th IEEE Symposium on Computers and Communications (ISCC'06), 2006.
- M. Bailey, E. Cooke, F. Jahanian, D. Watson, Jose Nazario, "The Blaster Worm: Then and Now," IEEE Security and Privacy, vol. 03, no. 4, pp. 26-31, 2005.
- C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram, D. Zamboni, "Analysis of a Denial of Service Attack on TCP," sp, p. 0208, 1997 IEEE Symposium on Security and Privacy, 1997.
- V. Paxson, "An analysis of using reflectors for distributed denial-of-service attacks" ACM SIGCOMM Computer Communication Review, 2001.
- M. Roesch, "Network Security: Snort - Lightweight Intrusion Detection for Networks", Proceedings of the 13th USENIX conference on System administration, November. 1999.
- T. H. Cormen, C. E. Leiserson, R. L. Rivest, "Introduction to Algorithms", p. p. 314-320, 1990.
- T. Ye, D. Veitch, G. Iannaccone and S. Bhattacharyya, "Divide and Conquer: PC-Based Packet Trace Replay at OC-48 Speeds", IEEE TRIDENTCOM, 2005.

- W. C. Feng, A. Goel, A. Bezzaz, W. C. Feng, and J. Walpole. "TCPivo: A high-performance packet replay engine". ACM SIGCOMM Workshop on Models, Methods and Tools for Reproducible Network Research (MoMeTools), Aug. 2003.
- R. W. Lucky, "Automatic equalization for digital communication," Bell Syst. Tech. J. , vol. 44, no. 4, pp. 547–588, Apr. 1965.

Index Terms

Computer Science Egovernance And Cloud Computing Services

Keywords

Ids Fps Fns Fp