{tag} {/tag}International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 141
-
Number 7

Year of Publication: 2016

Authors:

Isaac Bansah, Tonny Montana Adegboyega, Stephen Brako Oti

10.5120/ijca2016909709
{bibtex}2016909709.bib{/bibtex}

Abstract

The security of a Computer network cannot be compromised in any form as it would actually defeat the exact purpose for which the network exists; to provide connectivity between nodes that would allow exchange of information or resources. It also goes a long way to ensure absolute security for nodes in communication, information at source, in transit or flight and finally at the destination. Security implementations may vary according to network designs but it is essentially suppose to provide Authentication, Data integrity, Confidentiality, Access control and Availability. This paper looks at the implementation of an Intrusion Detection System on a Linux operating systems and analyzing the traffic, threats and vulnerabilities with a configured Firewall

General terms

Access privileges, Packets, Operating System

References

1. Ptacek, T. H. & Newsham, T. N. (1998). Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection [Online] Retrieved February 16, 2005 fromhttp://www.snort.org/docs/idspaper/

2. Kumar, S., (1995), Classification and Detection of Computer Intrusions. (Thesis).

3. Lunt, T. (1993). Detecting Intruders in Computer Systems [Online] Retrieved 25th March, 2005 from http://www.raptor.com/lib/canada93.ps

4. Roesch, M. (1999) Snort-Lightweight Intrusion Detection for Networks, Proceedings of LISA '99: 13th Systems Administration Conference [Online] Retrieved 10th April, 2005 fromhttp://www.usenix.org/publications/library/proceedings/lisa99/full_papers/roesch/roesch.pdf

5. Northcutt, S. and Novak, J., (2003), Network Intrusion Detection: An Analyst's Handbook, Third Edition. New Riders.

6. Northcutt, S. (2005) What is network intrusion detection? [Online] Retrieved 28th March, 2005 from http://www.sans.org/resources/idfaq/network_based.php

7. Allen, J. & Christie, A. (2000). "State of the practice of intrusion detection technologies" [Online] Retrieved February 20, 2005 from http://www.cert.org/archive/pdf/99tr028.pdf

8. Axelsson, S. "Intrusion detection systems: A survey and taxonomy," Technical Report 99-15, Department of Computer Engineering, Chalmers University, March 2000.

9. Burgess, M. (2004). Principles of Networking and System administration, (2nd Ed.). Chichester, John Wiley and Sons, Ltd.

10. Forrest, S., Hofmeyr, S. A., Somayaji, A. & Longstaff, T.A. (1996). "A Sense of Self for Unix Processes" Proceedings of the 1996 IEEE Symposium on Research in Security and Privacy [Online] Retrieved February 24, 2005 fromhttp://citeseer.ist.psu.edu/forrest96sense.html

11. Choi, M., (2008), Wireless Network Security. International Journal of Multimedia and Ubiquitous Engineering (Vol. 3, No. 3). School of Multimedia, Hannam University, Daejeon, Korea.

12. Nestler, V. J., et al., (2006), Computer Security Lab Manual. McGraw-Hill/Irwin, New York, USA.

13. Early, G (2004). Transmission Control Protocol (TCP), Lecture 04, University of Portsmouth.

14. Kurose, J.F. & Ross, K.W. Computer Networking: A Top- Down Approach Featuring the Internet, (2nd Ed.). Pearson Education, Inc.

15. Northcut, S. & Novak, J. (2002). Network Intrusion Detection, (3rd Ed.). New Riders Publishing.

Index Terms

Computer Science Information Sciences

Keywords

Intrusion Detection System, Linux, Traffic Analysis, Network Security