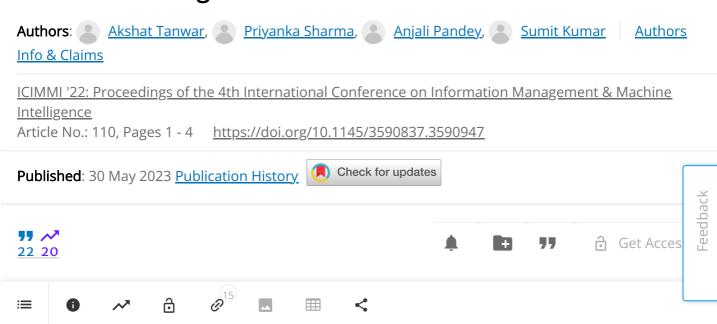


ICIMMI V

Intrusion Detection System Based Ameliorated Technique of Pattern Matching



Abstract

Intrusion Detection System is a set of programs that overlook both internal & external network operations. These IDS disinter skeptic patterns that expose a system attack from external variables (Hackers, Organizations, Government expose). The main function of IDS is to monitor a system and uncover malicious activity by generating alerts. These alerts or warnings get reported to a security operations center (SOC) analyst or incident responder who then takes appropriate action to rectify the threats. It enhances stability, surveillance, integrity, etc. of the user's system by protecting the user from network infiltrations. The more intrusions IDS detects, the better the detection rate is. IDS works on the multi-pattern matching method which can compete with the line–speed of pocket transfer. This method efficiently handles a range of patterns with variable pattern lengths. This article presents an approach that ventures to exceed efficacy in comparison to earlier



ICIMMI 🗸

References

- [1] P. Porras, D. Schnackenberg, "The Common Intrusion Detection Framework Architecture, CIDF", University of California, 1998.
 - **Google Scholar**
- [2] S.S. Sheik, sumit K aggarwal, Anindyapaddar, N. Balakrishnan, K Sekar, "A fast matching algorithm", J. Chem, Inf. Computer Sci., vol. 44, No. 4, 2004, Bangalore, India.

Show all references

Cited By

and Israni R. (2024). The Potential Future With ChatGPT Technology and AI Tools. Applications Challenges, and the Future of ChatGPT. 10.4018/979-8-3693-6824-4.ch013. (226-256). Online publication date: 28-May-2024.

https://doi.org/10.4018/979-8-3693-6824-4.ch013

Agarwal A, Trivedi A, Sharma P and Bhardwaj A. (2024). Use Cases of ChatGPT and Other AI Tools With Security Concerns. Applications, Challenges, and the Future of ChatGPT. 10.4018/979-8-3693-6824-4.ch012. (216-225). Online publication date: 28-May-2024.

https://doi.org/10.4018/979-8-3693-6824-4.ch012

Lalar S, Kumar T, Kumar R and Kumar S. (2024). Unveiling Privacy, Security, and Ethical Concerns of ChatGPT. Applications, Challenges, and the Future of ChatGPT. 10.4018/979-8-3693-6824-4.ch011. (202-215). Online publication date: 28-May-2024.

PDF



ICIMMI V

Recommendations

PGNIDS(Pattern-Graph based network intrusion detection system) design

ICCSA'06: Proceedings of the 2006 international conference on Computational Science and Its Applications - Volume Part III

PGNIDS(Pattern-Graph based Network Intrusion Detection System) generates the audit data that can estimate intrusion with the packets collected from network. An existing IDS(Intrusion Detection System), when it estimates an...

Read More

Building intrusion pattern miner for Snort network intrusion detection system

In this paper, we enhance the functionalities of Snort network-based intrusion detection system to automatically generate patterns of misuse from attack data, and the ability of detecting sequential intrusion behaviors. To that, we...

Read More

A Digest and Pattern Matching-Based Intrusion Detection Engine

Intrusion detection/prevention systems (IDSs/IPSs) heavily rely on signature databases and pattern matching (PM) techniques to identify network attacks. The engines of such systems often employ traditional PM algorithms to searc...

Read More

Comments

PDF Help

Join ACM



ICIMMI 🗸

Share Best Newest Oldest Nothing in this discussion yet.

Download PDF

View Table Of Contents

Categories	About
Journals	About ACM Digital Library PDF
Magazines	ACM Digital Library Board Help
Books	Subscription Information
Proceedings	Author Guidelines
SIGs	Using ACM Digital Library
Conferences	All Holdings within the ACM Digital Library
Collections	ACM Computing Classification System
People	Accessibility Statement
Join	Connect

https://dl.acm.org/doi/abs/10.1145/3590837.3590947#:~:text=Intrusion Detection System Based Ameliorated Technique of Pattern Matching,-Aksh...

Contact us via email



•

Suhmit a Rug Report

ICIMMI 🗸

The ACM Digital Library is published by the Association for Computing Machinery. Copyright © 2024 ACM, Inc.

Terms of Usage | Privacy Policy | Code of Ethics





PDF

Help