IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 6, April 2024

Intrusion Detection System

Aishwarya Londhe[1], Sahil Gawathe[2], Prathamesh Pandey[3], Gajanan Date[4], Sameer Meshram[5]

Faculty, Department of Computer Engineering[1]

Students, Department of Computer Engineering[2,3,4,5]

KC College of Engineering, Thane, India

Abstract: *Our project introduces an Integrated Intrusion Detection System (IDS) designed to bolster network and system security through a multi-faceted approach. This comprehensive IDS seamlessly combined Machine Learning, Anomaly Detection, File Scanning, and DDoS Prevention mechanisms to offer robust defense against diverse cyber threats. At the heart of the system lies the Machine Learning component, which continuously adapts to the evolving threat landscape. By analyzing network traffic and system behavior, it identifies both known and emerging threats in real-time, reducing reliance on traditional signature-based detection methods and allowing organizations to proactively stay ahead of cybercriminals. Anomaly Detection constantly monitors network and system activity, comparing it against established baselines. Any deviations from these baselines trigger alerts, facilitating swift responses to unusual activities that may indicate security breaches. File Scanning is another vital component ensuring data integrity and preventing malware infiltration or data exfiltration. It conducts thorough file analysis, checking for suspicious code, behavior, or unauthorized access, and offers continuous monitoring to detect anomalies in real-time. Additionally, our IDS includes Distributed Denial of Service (DDoS) Prevention mechanisms. By detecting and mitigating DDoS attacks, the system ensures the continuous availability of network resources and services even under intense traffic loads. This integrated approach to intrusion detection and prevention leverages Machine Learning, Honeypots, Anomaly Detection, File Scanning, and DDoS Prevention, empowering organizations to safeguard critical assets, maintain data integrity, and ensure network security in today's dynamic and perilous digital landscape. Our IDS solution serves as a valuable addition to the cybersecurity toolkit for organizations seeking comprehensive security against a wide range of threats.*

Keywords: Intrusion Detection System

REFERENCES

[1]. Anderson, B., & Lee, J. (2018). Intrusion Detection Systems with Machine Learning: A Review.Journal of Network and Computer Applications, 60, 19-31.

[2]. Cisco. (n.d.). Implementing Role-Based Access Control. Retrieved from https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_rbac/configuration/xe-16-12/s ec-user-rbac-xe-16-12-book/sec-rbac-xe-16-12-book.pdf

[3]. Kaspersky. (2020).APT Trends ReportQ1 2020. Retrieved from https://securelist.com/apt-trends-report-q1-2020/96264/

[4]. Krebs, B. (2018). DDoS Attacks Skyrocket. Retrieved from https://krebsonsecurity.com/2018/12/ddos-attacks-skyrocket/

[5]. Microsoft. (n.d.). Encrypt Files and Folders. Retrieved from https://support.microsoft.com/en-us/windows/encrypt-files-and-folders-5a6bf6f7-199b-4b 2a-a854-29c2d83b6e30

[6]. Panda Security.(2019). Types of Malware and How to Detect Them. Retrieved from https://www.pandasecurity.com/mediacenter/malware/types-malware-detect/

[7]. RFC Editor.(2017). Guidelines for Writing an IANA Considerations Section in RFCs.Retrieved from https://www.rfc-editor.org/rfc/rfc8126.txt

[8]. Stallings, W. (2017). NetworkSecurity Essentials: Applications and Standards (6th ed.). Pearson.

[9]. The Web Application Security Consortium. (n.d.). Web Appliation Firewall Evaluation Criteria. Retrieved

DOI: 10.48175/IJARSCT-17606