Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 1
Pages: 40-43

Enhancing Network Security through Log Analysis and Intrusion Detection Systems

Asad Vathare[1*]
Vishwakarma University, India
*Corresponding Author: Asad Vathare, 202000966@vupune.ac.in

Article history: Received: 25/05/2024, Revised: 29/05/2024, Accepted: 30/05/2024, Published Online: 31/05/2024

Abstract:
This research explores the enhancement of network security through log analysis and Intrusion Detection Systems (IDS). The study, based on an internship project, addresses the growing complexity of cyber threats and the need for effective security measures. It involves the practical implementation of IDS tools and log analysis platforms in a virtualized network environment. The paper discusses the project's rationale, methodology, results, and implications, emphasizing the critical role of proactive security measures in mitigating cyber threats.

Keywords: Log Analysis, Intrusion Detection Systems (IDS), Network Security, Network Monitoring

1. Introduction:

In the digital age, cyber threats are becoming increasingly sophisticated, necessitating robust security measures. Log analysis and Intrusion Detection Systems (IDS) are essential components of a comprehensive security strategy. Logs record events, actions, or messages generated by software, hardware, or users, providing crucial insights into system activities and potential security incidents. Log analysis is a critical component of modern network security and system management. In computing, logs are chronological records of events, actions, or messages generated by software, hardware, or users within a system. These logs provide a detailed account of system activities, capturing a wide range of information, including errors, warnings, informational messages, user actions, and system events. Effective log analysis allows organizations to monitor system performance, detect security incidents, and ensure compliance with regulatory requirements [1-3].

This paper outlines the types of logs, their significance, and the methodologies used to analyze them and detect intrusions.

- Types of Logs
    - System Logs: Record events related to the operating system, including startup and shutdown events, hardware events, and system errors.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 1
Pages: 40-43

- Application Logs: Generated by software applications, containing information about application activities, errors, warnings, and other relevant events.
- Security Logs: Capture security-related events such as login attempts, access control changes, and security policy violations.
- Web Server Logs: Produced by web servers, recording details about requests made to the server, including IP addresses, requested URLs, status codes, and user-agents.
- Database Logs: Track changes made to a database, such as inserts, updates, and deletes, as well as database errors and transactions.

2. Methodology:

Research and Selection of Tools

The project involved researching various IDS types and tools, understanding their functionalities, and selecting appropriate ones for implementation. Tools such as Snort, Suricata, Security Onion, and Splunk were chosen for their effectiveness in detecting and analyzing security threats.

Setting Up Network Topology

A virtualized network topology was designed using VMware to simulate real-world network environments. Virtual machines (VMs) were configured to represent different network components, including Security Onion, Splunk, pfSense, and Windows Server.

Installation and Configuration

Security Onion: Installed as the primary IDS solution, ensuring proper network monitoring and alerting.

Splunk: Set up for centralized log management and analysis, with data inputs and visualization dashboards configured.

pfSense: Configured as a router/firewall to control traffic flow within the network and enforce security policies.

Windows Server: Implemented Active Directory for user authentication and attack simulations

Log Capture and Analysis

Strategies were developed for capturing logs from various network devices and systems. Security Onion and Splunk were configured to collect and analyze logs, with data sources and correlation rules set up to identify patterns, anomalies, and potential security incidents.

Simulating Attacks

Simulated attack scenarios were conducted to test the effectiveness of IDS tools and response mechanisms. These included penetration testing, vulnerability assessments, and stress tests to evaluate the system's ability to detect and respond to security incidents.

3. Results:

Functional Testing

Functional testing ensured that each component of the system performed its intended functions correctly. The IDS tools successfully detected and alerted on predefined security events, while the log analysis platform effectively collected, parsed, and analyzed logs from different sources.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 1
Pages: 40-43

Performance Testing

Performance testing assessed the system's scalability and response time under normal and peak loads. The IDS tools and log analysis platforms maintained performance when processing logs and generating alerts, and network security devices handled high volumes of traffic efficiently.

Security Testing

Security testing verified the effectiveness of implemented security measures against common attack vectors and security threats. The system successfully detected and responded to simulated real-world attack scenarios, including malware infections, phishing attempts, and insider threats.

Integration Testing

Integration testing confirmed seamless communication and interaction between system components. Alerts generated by IDS tools were correlated with log data in the analysis platform, ensuring accurate detection and response to security incidents.

Usability Testing

Usability testing evaluated the user-friendliness of the system interfaces. Feedback from system administrators and security analysts indicated that the IDS consoles, log analysis dashboards, and network security device interfaces were intuitive and easy to navigate.

4. Discussion:

- Enhancing Network Security

  The project demonstrated that a well-designed and implemented IDS and log analysis system significantly enhances network security. By providing real-time insights into network activities and potential security incidents, these tools enable organizations to respond promptly and mitigate risks effectively.

- Challenges and Solutions

  Several challenges were encountered during the project, including the complexity of configuring and integrating different tools. These were addressed through thorough research, careful planning, and iterative testing, ensuring the system functioned optimally.

5. Conclusion

The internship project provided valuable insights and practical experience in enhancing network security through log analysis and IDS. By designing, implementing, and testing a comprehensive security infrastructure, the study highlighted the importance of proactive security measures, continuous monitoring, and rapid response in mitigating cyber threats. The findings underscore the critical role of IDS and log analysis in protecting organizational assets and ensuring operational resilience in the face of evolving cyber threats.

References:

1. Yeldi, S., Gupta, S., Ganacharya, T., Doshi, S., Bahirat, D., Ingle, R., & Roychowdhary, A. (2003, October). Enhancing network intrusion detection system with honeypot. In

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 1
Pages: 40-43

TENCON 2003. Conference on Convergent Technologies for Asia-Pacific Region (Vol. 4, pp. 1521-1526). IEEE.

2. Meryem, A., & Ouahidi, B. E. (2020). Hybrid intrusion detection system using machine learning. Network Security, 2020(5), 8-19.
3. Oliner, A., Ganapathi, A., & Xu, W. (2012). Advances and challenges in log analysis. Communications of the ACM, 55(2), 55-61.
4. Dhumane, A., Chiwhane, S., Mangore Anirudh, K., Ambala, S. (2023). Cluster-Based Energy-Efficient Routing in Internet of Things. In: Choudrie, J., Mahalle, P., Perumal, T., Joshi, A. (eds) ICT with Intelligent Applications. Smart Innovation, Systems and Technologies, vol 311. Springer, Singapore. https://doi.org/10.1007/978-981-19-3571-8_40
5. Dhumane, A.V., Kaldate, P., Sawant, A., Kadam, P., Chopade, V. (2023). Efficient Prediction of Cardiovascular Disease Using Machine Learning Algorithms with Relief and LASSO Feature Selection Techniques. In: Hassanien, A.E., Castillo, O., Anand, S., Jaiswal, A. (eds) International Conference on Innovative Computing and Communications. ICICC 2023. Lecture Notes in Networks and Systems, vol 703. Springer, Singapore. https://doi.org/10.1007/978-981-99-3315-0_52
6. Dhumane, A., and D. Midhunchakkaravarthy. "Multi-objective whale optimization algorithm using fractional calculus for green routing in internet of things." Int. J. Adv. Sci. Technol 29 (2020): 1905-1922.
7. Dhumane, A., Chiwhane, S., Tamboli, M., Ambala, S., Bagane, P., Meshram, V. (2024). Detection of Cardiovascular Diseases Using Machine Learning Approach. In: Garg, D., Rodrigues, J.J.P.C., Gupta, S.K., Cheng, X., Sarao, P., Patel, G.S. (eds) Advanced Computing. IACC 2023. Communications in Computer and Information Science, vol 2054. Springer, Cham. https://doi.org/10.1007/978-3-031-56703-2_14
8. Dhumane, A., Pawar, S., Aswale, R., Sawant, T., Singh, S. (2023). Effective Detection of Liver Disease Using Machine Learning Algorithms. In: Fong, S., Dey, N., Joshi, A. (eds) ICT Analysis and Applications. ICT4SD 2023. Lecture Notes in Networks and Systems, vol 782. Springer, Singapore. https://doi.org/10.1007/978-981-99-6568-7_15
9. A. Dhumane, S. Guja, S. Deo and R. Prasad, "Context Awareness in IoT Routing," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India, 2018, pp. 1-5, doi: 10.1109/ICCUBEA.2018.8697685.
10. Ambala, S., Mangore, A. K., Tamboli, M., Rajput, S. D., Chiwhane, S., & Dhumane, A. "Design and Implementation of Machine Learning-Based Network Intrusion Detection." International Journal of Intelligent Systems and Applications in Engineering, (2023), 12(2s), 120–131. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/3564
11. Kurle, A. S., & Patil, K. R. (2015). Survey on privacy preserving mobile health monitoring system using cloud computing. International Journal of Electrical, Electronics and Computer Science Engineering, 3(4), 31-36.
12. Meshram, V., Meshram, V., & Patil, K. (2016). A survey on ubiquitous computing. ICTACT Journal on Soft Computing, 6(2), 1130-1135.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 1
Pages: 40-43

13. Omanwar, S. S., Patil, K., & Pathak, N. P. (2015). Flexible and fine-grained optimal network bandwidth utilization using client side policy. International Journal of Scientific and Engineering Research, 6(7), 692-698.
14. Dong, X., Patil, K., Mao, J., & Liang, Z. (2013). A comprehensive client-side behavior model for diagnosing attacks in ajax applications. In 2013 18th International Conference on Engineering of Complex Computer Systems (pp. 177-187). IEEE.
15. Patil, K. (2016). Preventing click event hijacking by user intention inference. ICTACT Journal on Communication Technology, 7(4), 1408-1416.
16. Patil, K., Dong, X., Li, X., Liang, Z., & Jiang, X. (2011). Towards fine-grained access control in javascript contexts. In 2011 31st International Conference on Distributed Computing Systems (pp. 720-729). IEEE.
17. Patil, K., Laad, M., Kamble, A., & Laad, S. (2019). A Consumer-Based Smart Home with Indoor Air Quality Monitoring System. IETE Journal of Research, 65(6), 758-770.
18. Shah, R., & Patil, K. (2018). A measurement study of the subresource integrity mechanism on real-world applications. International Journal of Security and Networks, 13(2), 129-138.
19. Patil, K., & Braun, F. (2016). A Measurement Study of the Content Security Policy on Real-World Applications. International Journal of Network Security, 18(2), 383-392.
20. Patil, K. (2017). Isolating malicious content scripts of browser extensions. International Journal of Information Privacy, Security and Integrity, 3(1), 18-37.
21. Shah, R., & Patil, K. (2016). Evaluating effectiveness of mobile browser security warnings. ICTACT Journal on Communication Technology, 7(3), 1373-1378.
22. Patil, K. (2016). Request dependency integrity: validating web requests using dependencies in the browser environment. International Journal of Information Privacy, Security and Integrity, 2(4), 281-306.
23. Patil, D. K., & Patil, K. (2016). Automated Client-side Sanitizer for Code Injection Attacks. International Journal of Information Technology and Computer Science, 8(4), 86-95.
24. Patil, D. K., & Patil, K. (2015). Client-side automated sanitizer for cross-site scripting vulnerabilities. International Journal of Computer Applications, 121(20), 1-7.
25. Kawate, S., & Patil, K. (2017). An approach for reviewing and ranking the customers' reviews through quality of review (QoR). ICTACT Journal on Soft Computing, 7(2).
26. Jawadwala, Q., & Patil, K. (2016). Design of a novel lightweight key establishment mechanism for smart home systems. In 2016 11th International Conference on Industrial and Information Systems (ICIIS) (pp. 469-473). IEEE.
27. Patil, K., Vyas, T., Braun, F., Goodwin, M., & Liang, Z. (2013). Poster: UserCSP-user specified content security policies. In Proceedings of Symposium on Usable Privacy and Security (pp. 1-2).
28. Patil, K., Jawadwala, Q., & Shu, F. C. (2018). Design and construction of electronic aid for visually impaired people. IEEE Transactions on Human-Machine Systems, 48(2), 172-182.

Science Management Design Journal
Journal Homepage: www.smdjournal.com
ISSN: 2583-925X
Volume: 2
Issue: 1
Pages: 40-43

29. Kawate, S., & Patil, K. (2017). Analysis of foul language usage in social media text conversation. International Journal of Social Media and Interactive Learning Environments, 5(3), 227-251.
30. Patil, K., Laad, M., Kamble, A., & Laad, S. (2018). A consumer-based smart home and health monitoring system. International Journal of Computer Applications in Technology, 58(1), 45-54.
31. Meshram, V. V., Patil, K., Meshram, V. A., & Shu, F. C. (2019). An Astute Assistive Device for Mobility and Object Recognition for Visually Impaired People. IEEE Transactions on Human-Machine Systems, 49(5), 449-460.
32. Meshram, V., Patil, K., & Hanchate, D. (2020). Applications of machine learning in agriculture domain: A state-of-art survey. International Journal of Advanced Science and Technology, 29(5319), 5343.
33. Sonawane, S., Patil, K., & Chumchu, P. (2021). NO2 pollutant concentration forecasting for air quality monitoring by using an optimised deep learning bidirectional GRU model. International Journal of Computational Science and Engineering, 24(1), 64-73.
34. Meshram, V. A., Patil, K., & Ramteke, S. D. (2021). MNet: A Framework to Reduce Fruit Image Misclassification. Ingénierie des Systèmes d'Information, 26(2), 159-170.
35. Meshram, V., Patil, K., Meshram, V., Hanchate, D., & Ramteke, S. (2021). Machine learning in agriculture domain: A state-of-art survey. Artificial Intelligence in the Life Sciences, 1, 100010.
36. Meshram, V., & Patil, K. (2022). FruitNet: Indian fruits image dataset with quality for machine learning applications. Data in Brief, 40, 107686.
37. Meshram, V., Thanomliang, K., Ruangkan, S., Chumchu, P., & Patil, K. (2020). Fruitsgb: top Indian fruits with quality. IEEE Dataport.
38. Bhutad, S., & Patil, K. (2022). Dataset of Stagnant Water and Wet Surface Label Images for Detection. Data in Brief, 40, 107752.
39. Laad, M., Kotecha, K., Patil, K., & Pise, R. (2022). Cardiac Diagnosis with Machine Learning: A Paradigm Shift in Cardiac Care. Applied Artificial Intelligence, 36(1), 2031816.
40. Meshram, V., Patil, K., & Chumchu, P. (2022). Dataset of Indian and Thai banknotes with Annotations. Data in Brief, 108007.
41. Bhutad, S., & Patil, K. (2022). Dataset of Road Surface Images with Seasons for Machine Learning Applications. Data in Brief, 108023.
42. Pise, R., & Patil, K. (2022). Automatic Classification of Mosquito Genera Using Transfer Learning. Journal of Theoretical and Applied Information Technology, 100(6), 1929-1940.
43. Sonawani, S., Patil, K., & Natarajan, P. (2023). Biomedical Signal Processing For Health Monitoring Applications: A Review. International Journal of Applied Systemic Studies, 44-69.
44. Meshram, V., & Patil, K. (2022). Border-Square net: a robust multi-grade fruit classification in IoT smart agriculture using feature extraction based Deep Maxout

ISSN: 2583-925X
Volume: 2
Issue: 1
Pages: 40-43

network. Multimedia Tools and Applications, 81(28), 40709-40735.
45. Suryawanshi, Y., Patil, K., & Chumchu, P. (2022). VegNet: Dataset of vegetable quality images for machine learning applications. Data in Brief, 45, 108657.
46. Sonawani, S., & Patil, K. (2023). Air quality measurement, prediction and warning using transfer learning based IOT system for ambient assisted living. International Journal of Pervasive Computing and Communication, Emerald.
47. Meshram, V., Patil, K., Meshram, V., & Bhatlawande, S. (2022). SmartMedBox: A Smart Medicine Box for Visually Impaired People Using IoT and Computer Vision Techniques. Revue d'Intelligence Artificielle, 36(5), 681-688.
48. Meshram, V., Patil, K., Meshram, V., Dhumane, A., Thepade, S., & Hanchate, D. (2022). Smart low cost fruit picker for Indian farmers. In 2022 6th International Conference On Computing, Communication, Control And Automation (ICCUBEA) (pp. 1-7). IEEE.
49. Chumchu, P., & Patil, K. (2023). Dataset of cannabis seeds for machine learning applications. Data in Brief, Elsevier, 108954.
50. Meshram, V., Patil, K., & Bhatlawande, S. (2022). IndianFoodNet: Dataset of Indian Food images for machine learning applications. Data in Brief, 107927.
51. Meshram, V., Patil, K., & Ruangkan, S. (2022). Border-net: fruit classification model based on combined hierarchical features from convolutional deep network for Indian fruits. Multimedia Tools and Applications, 81, 4627-4656.
52. Meshram, V., & Patil, K. (2023). Border-Net: fruit classification model based on combined hierarchical features from convolutional deep network for Indian fruits. Multimedia Tools and Applications, 82, 22801-22830.
53. Patil, K., & Pise, R. (2023). Automation of coconut plantation system using sensors and wireless technology for smart agriculture. IETE Journal of Research.