Intrusion Detection Using Anomaly Detection Algorithm and Snort

- Chapter
- First Online: 08 February 2022
- pp 45–70
- Cite this chapter

Illumination of Artificial Intelligence in Cybersecurity and Forensics

- Chika Yinka-Banjo,
- Pwamoreno Alli,
- Sanjay Misra,
- Jonathan Oluranti &
- Ravin Ahuja

Part of the book series: Lecture Notes on Data Engineering and Communications Technologies ((LNDECT,volume 109))

- **722** Accesses
- **3** Citations

Abstract

Many organizations and businesses are all delving into crafting out an online presence for themselves. This could either be in the form of websites or

mobile apps. Many advantages come from an online presence; however, there are some drastic disadvantages that, if left unchecked, could disrupt any business or organization. Chief amongst these disadvantages is the aspect of security. However, many of the techniques that some organizations utilize to guard against unwanted access have been inadequate, and as a result, many unauthorized system break-ins have been reported. This is not made any better by the fact that certain applications used in hacking or system breach are now commonplace. Therefore, the focus of this work is to take an Intrusion Detection System (IDS) for a local network to detect network intrusion. A statistical approach, as well as a binomial classification, was used for simplicity in classification. The result shows the outlier value for each item considered; a 1 depicts an attack, a 0 depicts normalcy. The results are promising in dictating intrusion and anomalies in an IDS system.

This is a preview of subscription content, log in via an institution to check access.

Similar content being viewed by others

Intrusion Detection Systems (IDS)—An Overview with a Generalized Framework

Chapter © 2020

An Analytical Survey on Intrusion Detection System and Their Identification Methodologies

Chapter © 2019

A Systematic Study on Network Attacks and Intrusion Detection System

Chapter © 2022

References

1. Abdulbasit A, Alexei L, Clare D (2011) A misuse-based network intrusion detection system using temporal logic and stream processing. In: International conference on network and system security, pp 1–8

   Google Scholar

2. Aleksandar M, Marco V, Samuel K, Alberto A, Bryan DP (2017) Evaluating computer intrusions detection systems: a survey of common practices. Res Group Stand Perform Eval Corpor 48(1), Article 12. https://doi.org/10.1145/2808691

3. Alex D (2012) Intrusion detection using VProbes. Mass Inst Technol 1(2):28–31

   Google Scholar

4. Alia Y, Eric A (2018) Network intrusion dataset used in network security education. Int J Integr Technol Educ 7(3):43–50

   Article Google Scholar

5. Alireza H, Hossein S, Ahmad K (2006) A new framework: anomaly detection with snort intrusion detection system. In: Workshop on information technology and its disciplines

   Google Scholar

6. Bellovin SM (2001) Computer security—An end state? Commun ACM 44:131–132

   Article Google Scholar

7. Gopallkrishna NP, Kushank J, Nandan L, Narendra K, Yashasvi Z, Rohan S, Jyoti C (2014) Network intrusion detection system. Int J Eng Res Appl 4(4):69–72

   Google Scholar

8. Hamdan OA, Rafidah N, Zaidan BB, Zaidan AA (2010) Intrusion detection system. J Comput 2(2):130–133

   Google Scholar

9. Ibrahim K, Kemal H (2013) Open source intrusion detection system using snort. In: The 4th international symposium on sustainable development, pp 1–6

   Google Scholar

10. Jabez J, Muthukumar B (2015) Intrusion detection system (IDS): anomaly detection using outlier detection approach. Int Conf Intell Comput Commun Converg 48:338–346

Google Scholar

11. Jaiganesh V, Sumathi P, Vinitha A (2013) Classification algorithm in intrusion detection system: a survey. Int J Comput Technol Appl 4(5):746–750

Google Scholar

12. Lata KI (2013) Novel algorithm for intrusion detection system. Int J Adv Res Comput Commun Eng 2(5):2104–2110

Google Scholar

13. Lukasz S, Marcin G, Tomasz A (2013) Anomaly detection preprocessor for snort ids system. In: Image processing & communications challenges. Springer, Heidelberg, pp 225–232

Google Scholar

14. Manu B (2016) A survey on secure network: intrusion detection and prevention approaches. Am J Inf Syst 4(3):69–88. https://doi.org/10.12691/ajis-4-3-2

15. Mohammad JM, Mina S, Marjan KR (2010) Intrusion detection in database systems. Springer, Heidelberg, pp 93–101

Google Scholar

16. Mohit T, Raj K, Akash B, Jai K (2017) Intrusion detection system. Int J Tech Res Appl 5(2):38–44

Google Scholar

17. Muthu KR, Bala STV (2013) Intrusion detection system in web services. Int J Sci Res 2(2):224–228

Google Scholar

18. Naga SLM, Radhika Y (2018) Detection and analysis of network intrusions using data mining approaches. Int J Appl Eng Res 13(6):4059–4066

Google Scholar

19. Paresh G, Vishal G, Atish J, Sneha B (2018) Intrusion detection system using data mining. Int Res J Eng Technol 5(3):58–61

Google Scholar

20. Rahul Y, Kapil V (2017) Snort-J48 algorithm based intrusion detection and response system (IDRS) for cloud computing. Int J Res Sci Eng 3(2):465–470

Google Scholar

21. Rishabh G, Soumya S, Shubham V, Swasti S (2017) Intrusion detection system using snort. Int Res J Eng Technol 4(4):2100–2104

Google Scholar

22. Sahar S, Mohamed H, Taymoor NM (2011) Hybrid multi-level intrusion detection system. Int J Comput Sci Inf Secur 9(5):23–29

Google Scholar

23. Shivani A, Priyanka W, Shivam P, Sangram N, Sunil D (2020) Intrusion detection system. Int J Sci Res Sci Eng Technol 7(3):13–16. https://doi.org/10.32628/IJSRSET207293

24. Snehal B, Priyanka J (2010) Wireless intrusion detection system. Int J Comput Appl 5(8):975–8887

Google Scholar

25. Tanmay P, Piyush I, Omar K, Ashish N, Sheetal B (2017) Smart intrusion detection system. Int Res J Eng Technol (IRJET) 4(4):3404–3406

Google Scholar

26. Tariq A, Abdullah A (2014) Hybrid approach using intrusion detection system. Int J Comput Netw Commun Secur 2(2):87–92

Google Scholar

27. Vijayarani S, Maria SS (2015) Intrusion detection system—A study. Int J Secur Priv Trust Manag (IJSPTM) 4(1). https://doi.org/10.5121/ijsptm.2015.4104

28. Vinod K, Om PS (2012) Signature based intrusion detection system using snort. Int J Comput Appl Inf Technol I(III):35–40

Google Scholar

Download references

Author information

Authors and Affiliations

1. **Department of Computer Science, University of Lagos, Yaba, Lagos, Akoka, Nigeria**
   Chika Yinka-Banjo & Pwamoreno Alli
2. **Department of Computer and Communication, Østfold University College, Halden, Norway**
   Sanjay Misra
3. **Center of ICT/ICE, CUCRID, Covenant University, Ota, Nigeria**
   Jonathan Oluranti
4. **Shri Vishwakarma Skill University, Gurgaon, Hariyana, India**
   Ravin Ahuja

Corresponding author

Correspondence to Chika Yinka-Banjo .

Editor information

Editors and Affiliations

1. **Østfold University College, Halden, Norway**
   Sanjay Misra
2. **Computer Science and Engineering, Sri Sivasubramaniya Nadar College of Engineering, Chennai, Tamil Nadu, India**
   Chamundeswari Arumugam

Rights and permissions

Reprints and permissions

Copyright information

© 2022 The Author(s), under exclusive license to Springer Nature Switzerland AG

About this chapter

Cite this chapter

Yinka-Banjo, C., Alli, P., Misra, S., Oluranti, J., Ahuja, R. (2022). Intrusion Detection Using Anomaly Detection Algorithm and Snort. In: Misra, S., Arumugam, C. (eds) Illumination of Artificial Intelligence in Cybersecurity and Forensics. Lecture Notes on Data Engineering and Communications Technologies, vol 109. Springer, Cham. https://doi.org/10.1007/978-3-030-93453-8_3

Download citation

- .RIS
- .ENW
- .BIB

- DOIhttps://doi.org/10.1007/978-3-030-93453-8_3
- Published08 February 2022
- Publisher NameSpringer, Cham
- Print ISBN978-3-030-93452-1
- Online ISBN978-3-030-93453-8
- eBook PackagesIntelligent Technologies and RoboticsIntelligent Technologies and Robotics (R0)

Publish with us

Policies and ethics

Access this chapter

Log in via an institution

Chapter

EUR 29.95
Price includes VAT (Nigeria)

- Available as PDF
- Read on any device
- Instant download
- Own it forever

Buy Chapter

eBook

EUR 106.99

Softcover Book

EUR 129.99

Tax calculation will be finalised at checkout

Purchases are for personal use only

Institutional subscriptions

- Journals A-Z
- Books A-Z

165.73.223.224

Covenant University Ota (3006481499)

© 2024 Springer Nature