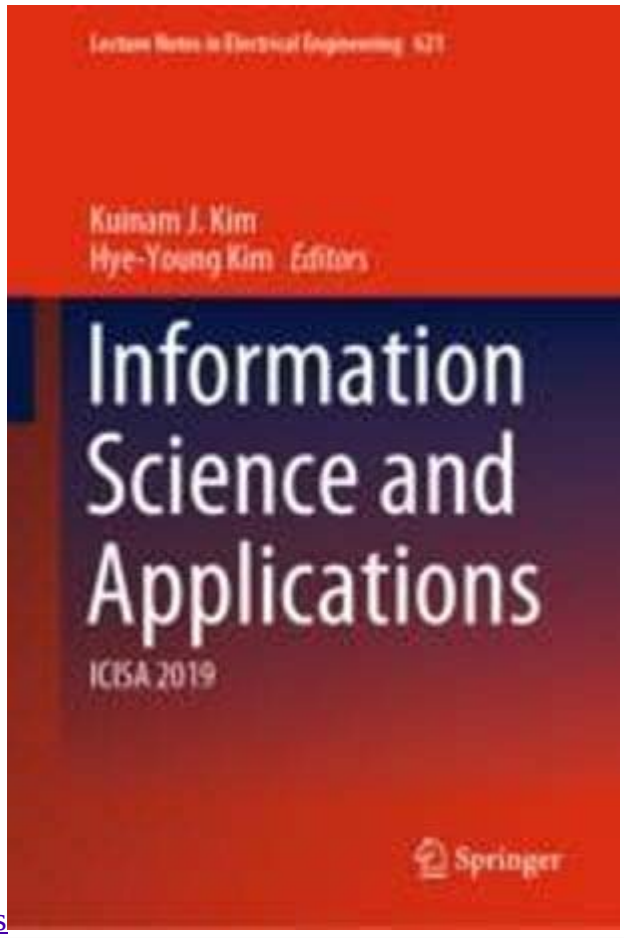
SpringerLink



Information Science and Applications
Information Science and Applications pp 73-83| Cite as

Mitigating Threats in a Corporate Network with a Taintcheck-Enabled Honeypot

- Authors
- Authors and affiliations
-
- Samuel Ndueso John
- Ola Ajibade Albert
- Kennedy Okokpujie
- Etinosa Noma-Osaghae
- Omoruyi Osemwegie
- Chinonso Okereke

Conference paper
First Online: 19 December 2019

Part of the Lecture Notes in Electrical Engineering book series (LNEE, volume 621)

Abstract

Conventional network security tools such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), anti-virus, antispyware and anti-malware integrated with firewalls generate a lot of false positives that make computer network system administration cumbersome. This paper proposes a novel mechanism comprising of taintcheck for dynamic analysis of buffer overflow attack using synthetic exploit and hybrid honeypot for scanning, detecting, identifying attackers and signature generation. In this framework, Noah's attack detection is used as a template. Upon testing, the practicality of the proposed framework was found to be more effective than other conventional network security tools as it effectively and comprehensively mitigates against threats and reported zero-day attacks with fewer false positives.

Keywords

Corporate networks Honeypot Security Threat Taintcheck Vulnerability Zero-day

Notes

Acknowledgements

This paper was sponsored by Covenant University, Ota, Ogun State.

References

1. 1.

Zeng Q, Kayas G, Mohammed E, Luo L, Du X, Rhee J (2018) Code-less patching for heap vulnerabilities using targeted calling context encoding. arXiv preprint arXiv:1812.04191

2. 2.

Arefi MN, Alexander G, Crandall JR (2018) PIITracker: automatic tracking of personally identifiable information in windows. In: Proceedings of the 11th european workshop on systems security. ACM, p 3Google Scholar

3. 3.

Okokpujie K, Shobayo O, Noma-Osaghae E, Imhade O, Okoyeigbo O (2018) Performance of MPLS-based virtual private networks and classic virtual private networks using advanced metrics. Telkomnika 16(5):2073–2081CrossRefGoogle Scholar

4. 4.

Okokpujie K, Emmanuel C, Shobayo O, Noma-Osaghae E, Okokpujie I (2019) Comparative analysis of the performance of various active queue management techniques to varying wireless network conditions. Int J Electr Comput Eng (IJECE) 9(1):359–368CrossRefGoogle Scholar

5. 5.

John SN, Ndujiuba CU, Okonigene RE, Okereke CE, Wakama ME () Creating a policy based network intrusion detection system using java platform. In: Regular research paper (RRP). The 2014 world congress in computer science, computer engineering, and applied computing (WORLDCOMP'14), annual summer international conference on security and management (SAM'14: 21–24 July 2014), USA, pp 319–324Google Scholar

6. 6.

Okokpujie KO, Chukwu EC, Noma-Osaghae E, Okokpujie IP (2018) Novel active queue management scheme for routers in wireless networks. Int J Commun Antenna Propag (IRECAP) 8(1):53–61CrossRefGoogle Scholar

7. 7.

Portokalidis G, Bos H (2007) Eudaemon: a good spirit to protect processes from Internet attacks. Technical report. Department of Computer Science Vrije Universiteit AmsterdamGoogle Scholar

8. 8.

Yin H, Song D (2006) Whole-system fine-grained taint analysis for automatic malware detection and analysis. Technical paper. College of William and Mary & Carnegie Mellon UniversityGoogle Scholar

9. 9.

Wang P, Chao K-M, Lo C-C, Lin W-H, Lin H-C, Chao W-J (2016) Using malware for software-defined networking–based smart home security management through a taint checking approach. Int J Distrib Sens Netw 12(8):1550147716662947Google Scholar

10. 10.

Newsome J, Song DX (2005) Dynamic taint analysis for automatic detection, analysis, and signature generation of exploits on commodity software. In NDSS, vol. 5. Citeseer, pp 3–4Google Scholar

11. 11.

Marhusin MF (2012) Improving the effectiveness of behaviour-based malware detection. University of New South Wales, Canberra, AustraliaGoogle Scholar

12. 12.

Bosman E, Slowinska A Bos H (2011) Minemu: the world's fastest taint tracker. In International workshop on recent advances in intrusion detection, pp 1–20. SpringerGoogle Scholar

Copyright information

About this paper

CrossMark

Cite this paper as:

John S.N., Albert O.A., Okokpujie K., Noma-Osaghae E., Osemwegie O., Okereke C. (2020) Mitigating Threats in a Corporate Network with a Taintcheck-Enabled Honeypot. In: Kim K., Kim HY. (eds) Information Science and Applications. Lecture Notes in Electrical Engineering, vol 621. Springer, Singapore

- **First Online**19 December 2019
- **DOI**https://doi.org/10.1007/978-981-15-1465-4_8
- **Publisher Name**Springer, Singapore
- **Print ISBN**978-981-15-1464-7
- **Online ISBN**978-981-15-1465-4
- **eBook Packages**Engineering
- Buy this book on publisher's site
- Reprints and Permissions