Penetration testing using Kali Linux: SQL injection, XSS, Wordpress, and WPA2 attacks

Gunawan, T.S.¹, Lim, M.K.², Kartiwi, M.³, Malik, N.A.³, Ismail, N.⁴

¹Electrical and Computer Engineering Department, International Islamic University Malaysia, Malaysia
²Information Systems Department, International Islamic University Malaysia, Jalan Gombak, Kuala Lumpur, 53100, Malaysia
³Electrical Engineering Department, Faculty of Science and Technology, UIN Sunan Gunung Djati, Jalan A.H. Nasution 105, Bandung, Indonesia

Abstract

Nowadays, computers, smart phones, smart watches, printers, projectors, washing machines, fridges, and other mobile devices connected to the Internet are exposed to various threats and exploits. Of the various attacks, SQL injection, cross site scripting, Wordpress, and WPA2 attack were the most popular security attacks and will be further investigated in this paper. Kali Linux provides a great platform and medium in learning various types of exploits and penetration testing. All the simulated attack will be conducted using Kali Linux installed on virtual machine in a computer with Intel Core i5 and 8 GB RAM, while the victim's machine is the host computer which run Windows 10 version 1709. Results showed that the attacks launched both on web and firewall were conducted successfully. © 2018 Institute of Advanced Engineering and Science. All rights reserved.

Author keywords

Cross site scripting, Kali Linux, SQL injection, Wordpress attack, WPA2 attack

Funding details

Funding number | Funding sponsor | Acronym | Funding opportunities
--- | --- | --- | ---
RIGS15-070-0070 | International Islamic University Malaysia | IIUM | |

Funding text

The researchers in this study would like to acknowledge the International Islamic University Malaysia (IIUM) for the financial funding of this research through the Research Initiatives Grant Scheme (RIGS) RIGS15-070-0070.

References (14)

View in search results format
1. Shinde, P.S., Ardhapurkar, S.B. (2016). Cyber security analysis using vulnerability assessment and penetration testing. *IEEE WCTFTR 2016 - Proceedings of 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare*, art. no. 7583912. Cited 7 times. ISBN: 978-146739214-3 doi: 10.1109/STARTUP.2016.7583912

2. Halfond, W.G., Viegas, J., Orso, A. (2006). A classification of SQL-injection attacks and countermeasures. *Proceedings of the IEEE International Symposium on Secure Software Engineering*, pp. 13-15. Cited 138 times.

3. Appelt, D., Nguyen, C.D., Briand, L.C., Alshahwan, N. (2014). Automated testing for SQL injection vulnerabilities: An input mutation approach. *2014 International Symposium on Software Testing and Analysis, ISSTA 2014 - Proceedings*, pp. 259-269. Cited 26 times. ISBN: 978-145032645-2

4. Dayal, M., Singh, N., Raw, R.S. (2016). A comprehensive inspection of cross site scripting attack. *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016*, art. no. 7813770, pp. 497-502. Cited 2 times. ISBN: 978-150901666-2 doi: 10.1109/CCAA.2016.7813770

5. Kyaw, A.K., Sioquim, F., Joseph, J. (2015). Dictionary attack on Wordpress: Security and forensic analysis. *2015 2nd International Conference on Information Security and Cyber Forensics, InfoSec 2015*, art. no. 7435522, pp. 158-164. Cited 5 times. ISBN: 978-146736988-6 doi: 10.1109/InfoSec.2015.7435522

6. Denis, M., Zena, C., Hayajneh, T. (2016). Penetration testing: Concepts, attack methods, and defense strategies. *2016 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2016*, art. no. 7494156. Cited 10 times. ISBN: 978-146738490-2 doi: 10.1109/LISAT.2016.7494156

7. Allen, L., Heriyanto, T., Ali, S. (2014). *Kali Linux–Assuring Security by Penetration Testing*. Cited 3 times. Packt Publishing Ltd