Topic ID: 198-IT-EN

Advanced Penetration Testing of Web Applications Vulnerabilities with Open Source Applications Based on OWASP

Supervisor: Prof. Ing. Šenkeřík Roman, Ph.D.

Consultant: Ing. Malaník David, Ph.D., ---

Department: Department of Informatics and Artificial Intelligence

Programme: Information Technologies

Abstract:

Currently, the number of Web applications are increasing continuously every day together with more or less successful attacks on these applications. Many tools are used for penetration testing to eliminate vulnerabilities. The proposed research will examine, analyze, and compare in details broad portfolio of open source tools for penetration testing of web applications vulnerabilities based on OWASP (Open Web Application Security Project) guidelines. The aim of the thesis will also be to analyze real incidents from recent years and to evaluate whether testing, according to OWASP, could help prevent these incidents. Thus, how to further improve penetration testing and how to use the correlation of output from many different tests to create more complex models (with the possible use of A.I.).

Literature:

[1] KENNEDY, David. Metasploit: the penetration tester's guide. San Francisco: No Starch Press, c2011. ISBN 9781593272883.

[2] TEVAULT, Donald A., 2018. Mastering Linux Security and Hardening. 1. Packt Publishing Limited. ISBN 9781788620307.

[3] SAK, Brian a Jilumudi Raghu RAM, 2016. Mastering Kali Linux Wireless Pentesting. 1. Packt Publishing. ISBN 9781785285561.

[4] BLOKDYK, Gerardus, 2019. OWASP A Complete Guide - 2019 Edition. 1. 5STARCooks. ISBN 978-0655539032.

[5] ALLEN, Lee a Kevin CARDWELL, 2016. Advanced Penetration Testing for Highly-Secured Environments - Second Edition. 2. ISBN 9781784395810.