

Strategies for Monitoring Websites Security against Cyber-Attacks

Ioan-Cosmin MIHAI¹, Ray GENOE², Ștefan PRUNĂ¹

¹ "Alexandru Ioan Cuza" Police Academy, Bucharest, Romania

² UCD Centre for Cybersecurity & Cybercrime Investigation, Ireland

cosmin.mihai@academiadepolitie.ro, ray.genoe@ucd.ie, stefan.pruna@academiadepolitie.ro

Abstract

To secure a website you need to engage in three strategies: prevention (before an attack), detection (during an attack) and response (after an attack). To study the effects of cyber-attacks on a website we developed an attack tree, which is useful to explore certain attack paths in depth and to generate intrusion scenarios. The results were used to presents strategies for monitoring websites security against cyber-attacks.

Index terms: cybersecurity, website security, cyber-attacks, malware

References:

- [1]. Majority Staff Report, A "Kill Chain" Analysis of the 2013 Target Data Breach, 2014.
- [2]. E.M. Hutchins, M.J. Clopperty, and R.M. Amin, Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, 2011.
- [3]. B. Schneier, Attack Trees: Modeling Security Threats, Dr. Dobb's Journal, 2003.
- [4]. J.A. Lewis. Holistic Approaches to Cybersecurity to Enable Network Centric Operations, 2008.
- [5]. Cybersecurity, (2014, Apr. 13), [Online] Available: <http://www.securitatea-cibernetica.ro/>
- [6]. Detect Website Malware, (2014, Apr. 22), [Online] Available: <https://sucuri.net/website-antivirus/malware-scanning-and-detection>
- [7]. Cookie Checker, (2014, Apr. 24), [Online] Available: <http://www.cookie-checker.com>