A Study on Password Strength in Wireless Encryption Protocols

Gabriel PETRICĂ
EUROQUALROM - ETTI, University "Politehnica" of Bucharest, Romania
gabriel.petrica@upb.ro

Abstract

Solutions that can be implemented to secure a LAN include firewalls and intrusion detection / prevention systems (IDS / IPS). For a wireless network, security is a challenge considering the specific elements of this type of network: the physical area from which the connection is possible, and the weaknesses of the protocols used for data encryption. This article presents a case study on the most widely used protocols (WEP, WPA and WPA2) to secure wireless networks and the methodology by which passwords can be decrypted using Kali Linux distribution - available for free on the Internet - and applications included in this operating system.

Index terms: WPA, WPA2, encryption, password strength, wireless networks

References:

[1]. 802.11-2016 - IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7786995

[2]. US Department of Homeland Security - Wireless Local Area Network (WLAN) Reference Architecture v.1, 2011.

[3]. R. Thubron, WPA3 protocol will make public Wi-Fi hotspots a lot more secure, Techspot, https://www.techspot.com/news/72656-wpa3-protocol-make-public-wi-fi-hotspots-lot.html.

[4]. Kali Linux Documentation, https://www.kali.org/kali-linux-documentation/.

[5]. E. Tews, R.P. Weinmann, A. Pyshkin, Breaking 104 bit WEP in less than 60 seconds, WISA, Lecture Notes in Comp. Sc., 4867, pp. 188-202, Springer, 2007.

[6]. CERT-RO, Ghid de securitate informatică pentru funcționarii publici, cert.ro/citeste/update-ghidul-de-securitate-informatica-functionarii-publici-v-1-1.