

PENETRATION TESTING IN WI-FI NETWORKS

SHORUNKE MUYIWA MUSADDIQ

Department of Mathematics & Computer Science, Elizade University Ilara-Mokin, Ondo State, Nigeria

ABSTRACT

Wi-Fi network connection access points are easily discovered all around us today through the use of any free Wi-Fi discovery tool made available free on the web, also with the aid of common hardware such as laptops that are Wi-Fi enabled. Its usage ranging from private to corporate and public use, has made it a favourable target for attacks by black hat hackers. Unfortunately, most Wi-Fi network users do not see the significance and effectiveness of conducting security audits routinely in order to fortify their network and to detect how weak and vulnerable their Wi-Fi network is to malicious attacks. Although conducting a proper penetration test on a Wi-Fi network can be tasking and quite expensive, but its value cannot be underestimated. Unlike most private users, corporate users often do carry out security audits (i.e. Penetration Tests) so as to protect their web-based assets. This paper looks into the various types of attacks faced by Wi-Fi network users, particularly the private users. The paper further highlight most security weakness encountered on private Wi-Fi network with simple network penetration test conduct. Finally, the papers suggests and propose simple and less expensive countermeasures that Wi-Fi private users can employ to properly secure and improve the quality of performance the Wi-Fi network connection access.

KEYWORDS: Wi-Fi Network, Penetration Test, Security, WEP, WPA, Denial of Service (Dos), WPA2