Abstract

Extensible Authentication Protocol (EAP) was designed to provide a general structure for several different authentication methods. IEEE 802.1X uses EAP as an authentication tool. The IEEE 802.1X standard defines a client-server authentication and access control protocol that restricts unauthorized users from connecting to a network. This paper aims at using penetration testing to conduct security assessment of some IEEE 802.1x Port-Based Authentication protocols (PEAP, EAP-TTLS and Inner Authentication Method MSCHAPv2 and PAP). Vulnerabilities identified were exploited using Kali Linux with its Aircrack-ng tools.

References


NIST Special Publication 800-120, September 2009.


Index Terms

Computer Science Wireless

Keywords

IEEE 802.1x, EAP, PEAP, TTLS, PAP, MSCHAPv2, Penetration Testing, Wireless Network, WLAN, Kali Linux