Abstract

Many OS identification methods had been used to accurately identify the remote OSes that are running over remote machines. OS identification is considered to be the primary step that is taken by attackers trying to penetrate a targeted network machines. Thus, it will be useful for system and network administrators to be up to date with the latest information about their systems and networks remotely. In this paper, a survey on operating system identification main techniques; the active and the passive are discussed and analyzed. This study will first identify the existing OS identification methods and tools. Furthermore, it will test and analyze these methods and tools. Operating system identification (fingerprinting) is the art of detecting the operating system that is running on a remote machine (i.e. Windows, Linux...) depending on the operating system tcp stack fingerprint. OS fingerprint is a combination of OS's tcp stack parameters. Window Size (WS), Time To Live (TTL), Maximum Segment Size (MSS), Don't Fragment Bit (DF) and TCP options are OS dependant parameters; that is why it can be used to distinguish between the operating systems.