

## Netware Penetration Testing Overview

Despite being an unorthodox operating system and a cross between the Linux and Windows operating environments, Novell Netware does have some inherent security flaws that make exploiting the operating system is fairly easy, especially with the older Netware 4 and Netware 5.0 Operating Systems. There are very few “script kiddy” type attacks however as outlined in the 4<sup>th</sup> edition of Hacking Exposed, all that is required is a moderate level of skill and experience with introductory level penetration testing.

Although Novell like any other operating system is responsible to its customers to provide a secure environment, its support life cycle for Netware is fast ending. Indeed with Netware 4 and 5 there are currently no support packs offered and Netware 5.1 is scheduled to be phased out before the end of the year. Having mentioned the support life cycle 80% of all Netware administrators do not update there systems on a regular basis, Novell offers no automatic update and support packs installation is often a tedious and difficult process, for that reason a number of Netware servers are left vulnerable to the types of attacks outlined in this article.

Additionally as mentioned in the Netware risk management article, a number of Netware systems are generational in nature meaning that there deployment schedule is over a great period of time, for instance if a Netware 5 server was deployed in a typical environment it would be between 7 and 10 years before the server was evaluated for a update, and more often then not the Netware server would be migrated to a newer version of Netware or additionally servers be installed to not compromise the existing e-directory.

This article will outline Network Oriented escalation of privileges attacks on Netware 5 & 6 Servers as well as denial of service and social engineering attacks, outlined by the majority of Netware users as being there greatest security problems or concerns.