Abstract

Signature-based input filtering is an important and widely deployed mechanism for defense against Internet worms. However the traditionally used signatures which are basically exploit based have limited coverage and can be easily evaded by polymorphic worm attacks with small variations of the exploit message.

Recently, there have been proposals for a new form of signature called Vulnerability Signature that is based on the vulnerable program itself rather than on the instances of worm exploits. These have the potential to protect a network from any worm attack that exploits a known vulnerability. Particularly, the Protocol-level vulnerability signatures are compact, have high coverage and can guarantee zero false positive and zero false negative

In this project we develop a filtering engine for the deployment of protocol level vulnerability signatures at the edge router for an enterprise network. To write the filtering engine we have used Linux Kernel Modules which is basically a chunk of codes we can add to the Linux Kernel while it is running thus giving it the name loadable kernel module. They basically form an extension of the Linux Kernel and run in the kernel space of the Operating System. For the testing we have implemented the filter in a simulated VMware environment. The attacks were generated by running worm codes as well as through Metasploit.