Abstract

The alarming rise in the number of computer security incidents since the late 80's had inspired researchers to devise new mechanisms for detection and containment of malwares like worms and viruses. Traditional approaches like worm signatures are helpless against new age polymorphic and metamorphic worms. Design and implementation of an anomaly based detection system seems is a herculean task due to the difficulty in defining a normal model.

Signature based systems match the incoming traffic against a signature database. The effectiveness of any filtering engine depends on the coverage of the deployed signatures. Recent work shows that protocol level vulnerability signatures offers much higher coverage. In this project, we make an attempt to develop a packet filtering engine for deployment of protocol level vulnerability signatures. This was done with the help of netfilter which is a packet filtering sub-system in the Linux kernel. Netfilter allows parsing of the application layer protocol, which is required for deployment of protocol level signatures.

The signatures were deployed and tested in VMware environment. Experimental results indicate zero rates of false positives and false negatives. Hence in this project we accomplished an effective mechanism for deployment of protocol level vulnerability signatures.