Abstract

Slowdown in the network performance can cause serious concern to network analysts, leading to loss in resources. Such cases are not easy to deal with, due to the lack of time and resources available. Lack of awareness about appropriate tools which detect the attacks or not knowing exactly why a loss in network performance is occurring are some other factors. Connectivity loss or shutting down of terminals within the network for unknown reasons are among the other problems. Mostly, the cause of these problems cannot be detected accurately and is concluded due to poor network architecture, such as inefficiently configured broadcast storms, spanning-tree, usage of unsuitable routing protocols within the network domain, redundant links etc. However, sometimes the cause could be due to attacks by unknown third parties that try to put the web server out-of-service through means of a DoS (Denial of Service) attack, sending traffic with a poisoned ARP in an attempt to discover hosts to infect, or by simply infecting ports with malware to form part of an alien network or botnet. In all these cases, knowing the source of the attack is the first step towards taking appropriate action and achieving correct protection. That is when packet sniffers can be extremely useful to detect, analyze and map traffic. Such packet sniffers identify threats to the network and limit their harmful consequences.
References

- 2010 18th IEEE Symposium on High Performance Interconnects Innovating in Your Network with OpenFlow: A Hands-on Tutorial
- 2011 Fourth International Joint Conference on Computational Sciences and Optimization: Application Design of Data Packet Capturing Based on SharpCap
- IEEE 2008 publication: Bottleneck Analysis of Traffic Monitoring using Wireshark

Index Terms

Computer Science
Networks
Keywords
Packet sniffing tools  Wireshark  LAN attacks