Abstract

Network sniffing was considered as a major threat to network and web application. Every device connected to the Ethernet-network receives all the data that is passed on the segment. By default the network card processes only data that is addressed to it. However listening programs turn network card in a mode of reception of all packets – called promiscuous mode. So, a sniffer is a special program or piece of code that put the Network Interface Card (NIC) in
Sniffing: A Major Threat to Secure Socket layer and its Detection

the promiscuous mode. When NIC works in promiscuous mode, the user of that system can steal all the data including password etc. without generating any traffic. Any network system running the sniffer can see all the data movement over the network. Many sniffers like wireshark, Cain & Abel, ethersniff etc. are available at no cost on the internet. There are many proposed solutions are available for the detection of network sniffing including antisniff [1], SnifferWall [2], Sniffer Detector [3] etc. but any solution does not guarantee full security. Due to this reason many new techniques were developed including secure socket layer (https), one time password etc. but now there are some techniques that can be used to sniff this secure data. In this paper we are discussing different aspects of sniffing, methods to sniff data over secure socket network and detection of sniffer. The paper describes all the technical details and methods to perform this task. The Address Resolution Protocol packets are used to query hardware addresses from IP addresses. We are using this fact to verify to whether the NIC’s are set to promiscuous mode. When NIC receiving all packets, it will not block any packet and forwards it to the kernel for further processing. Now according to the working of the ARP, the kernel may make mistake by responding to some packets that it is not supposed to respond. So according to this mechanism we can compose fake ARP request packets and send them to every node on the network. If any node responds to this fake request, we can detect it is running in promiscuous mode.

References

- Thawatchai Chomsiri, Sniffng packets on lan without arp spoofing, Third 2008 International Conference on Convergence and Hybrid Information Technology(2008).
- D. Wu and F. Wong, Remote sni_er detection, Computer Science Division, University of California, Berkeley (1998).
- www.evsslcertificate.com/ssl/description-ssl.html
- S. Grundschrober, Sni_er detector report, IBM Research Division, Zurich Research Laboratory, Global Security Analysis Lab (1998).

Index Terms

Computer Science
Communication and Networks
Keywords

Keywords are your own designated keywords which can be used for easy location of the manuscript using any search engines.