Sniffer Detection Techniques: A Review

Amit Mishra[1#], Prof. (Dr.) Ajay Mathur[2]
Ph.D. Scholar[1] and Associate Professor[#]
Dept. of CSE
Career Point University Kota, India[1]
JIET Jodhpur[#]
Professor and Head, Govt. Polytechnic College Jodhpur[2]

Abstract: - **Network threats can be divided into two major categories as internal threat and external threat. Sniffer is a program that comes under the category of internal threats. Detection of Internal threat is difficult as the intruder or hacker is from the same network and having knowledge of security configurations and policies. Many approaches and solutions are available for sniffer detection. Here in this paper we are discussing different approaches with their pros and cons.**

I. INTRODUCTION

Network sniffing can be 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 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. [1]

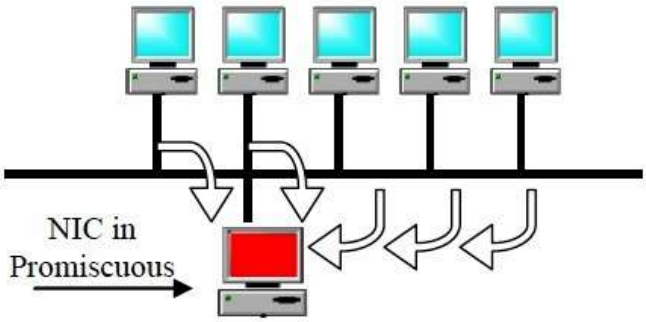

Figure 1. NIC working in Promiscuous Mode

II. SNIFFER DETECTION TECHNIQUES

Many researchers and researches have contributed by proposing solutions and ways for sniffer detection in a network. Securing the information within an organization is a tricky part, especially in internal threats when network nodes are prone to sniffing. H. AbdelallahElhadj H. M. Khelalfa and H. M. Kortebi (H. AbdelallahElhadj et al. 2002), known as SnifferWall, utilizes MAC-based and Deception or Decoy-based methods. In the MAC- based detection, this method uses “Etherping Test” and “ARP Test” for sniffer detection. The decoy method is based on the concept of deceit or honeypot. The idea is to design a tool which allows spreading out bait (false passwords, false user names), which are supposed to be especially attractive for the sniffer owner and await him to launch an attack by reusing the fake information spread out (knowing that nobody except sniffer owner knows these false passwords) [2]. The architecture of proposed system can represented as follows in diagram:-

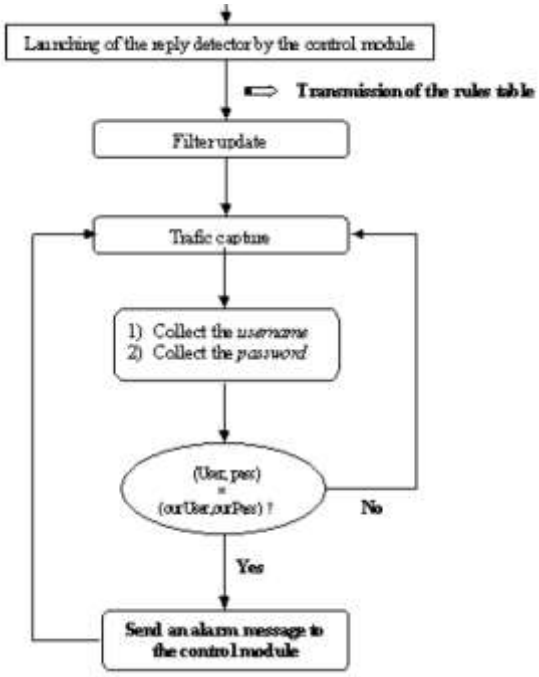

Figure2. Architecture of SnifferWall [2]

The proposed method works fine but it cannot be used to detect sniffer if the intruder is running MAC spoofing softwares or can change the IP address of the system. Z. Trabelsi, H. Rahmani, K. Kaouech and M. Frikha (Z. Trabelsi et al. 2004) suggested sniffer detection using ARP (Address Resolution Protocol) request packets. In this method ARP packets with fake hardware address are sent to suspicious host or in the complete network. As all the nodes not working as a sniffer will ignore this message, but only host running sniffer program will respond to this false ARP request [3]. So network administrator can detect this response and identifies the sniffer running on a particular host. Although this approach is useful and efficient but it has some drawbacks also. If we have access to the OS architecture and can modify the basic behaviour of OS, then this approach will not work. In the next approach, Deepak D. Kshirsagar, Sachin S. Sale, Dinesh K. Tagad and Ganpat Khandagale (Deepak D. Kshirsagar et al. 2011) suggested intrusion detection system containing five modules named: Capture Module, Decode Module, Detection Module, Known Attack Pattern Module and Action Module [4]. This is an efficient technique but it is a little bit complex and it also depends on the known attacks. It is basically pattern based IDS (intrusion detection system) that focuses on packet sniffer and its working.

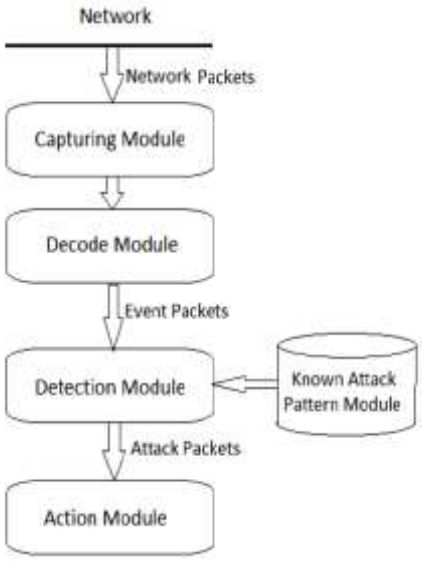

Figure3. Architecture of CDDA model for IDS [4]

Indeed, few remotely based sniffer detector have been developed the two most famous tools are the two most famous tools for sniffer detection are: AntiSniff [5] (Windows platform) developed by l0pht Heavy Industries, and SNIFFER DETECTOR (Linux platform) developed by IBM-Zurich [6]. The disadvantage of AntiSniff is that it can significantly degrade network performance. Furthermore, packets can be delayed simply because of the load on the wire, which may cause timeouts and therefore false positives [8].

CONCLUSION

Widespread of technology and advancement in networks has out-casted the predominance of numerous interconnected, interdependent and interrelated machines and networks. Though, the intrusion occurrences stay identical and consistent irrespective of network terminology. Sniffing is considered as a major threat to network security, as it does not generates any traffic. Instead of generation, Sniffer is designed to collect all the network traffic in the form of packets. This has waved various sniffing intrusion detection techniques in central as well as distributed system networks. The abovementioned techniques of sniffer detection are working with some predefined constraints and having other limitation also. So new approaches with emerging technologies like cloud computing, mobile agents etc. should be derived for sniffer detection.

REFERENCES

[1] Ajay Mathur, Sudhir Kr.Sharma, Amit Mishra. (2011) “Sniffing: A Major Threat to Secure Socket layer and its Detection” Proceedings of the International Conference on Computer Communication and Networks CSI- COMNET-2011, published by IJCA.
[2] H. AbdelallahElhadj H. M. Khelalfa and H. M. Kortebi (H. AbdelallahElhadj et al. 2002) “An Experimental Sniffer Detector: SnifferWall”
[3] Z. Trabelsi, H. Rahmani, K. Kaouech and M. Frikha (Z. Trabelsi et al. 2004) “Malicious sniffing systems detection platform” IEEE Applications and the Internet, 2004, pp. 201-207
[4] Deepak D. Kshirsagar, Sachin S. Sale, Dinesh K. Tagad and Ganpat Khandagale (Deepak D. Kshirsagar et al. 2011) published in IEEE as proceedings of Electronics Computer Technology (ICECT), 2011 3rd International Conference, volume 5 , pp. 283-286
[5] https://packetstormsecurity.com/sniffers/antisniff/
[6] S. Grundschober. Sniffer Detector report. Diploma Thesis, IBM Research Division, Zurich Research Laboratory, Global Security Analysis Lab, June 1998
[7] D. Wu and F. Wong. Remote Sniffer Detection. Computer Science Division, University of California, Berkeley. December 14, 1998