NetCap: A Packet Sniffer in Java

[1]Rajan Parmar, [2]Hetal Patel
[1,2]Nirma University, Ahmedabad, India

Abstract

A packet sniffer is a wiretap device that plugs into computer networks; unlike telephone circuits, computer networks are shared communication channels. Sharing means that computers can receive information that was intended for other machines (HUB). NetCap is a type of packet sniffer software that captures the network data as well as provides sufficient means for decision making process of administrator. This paper illustrates NetCap and its benefits over existing packet sniffers. NetCap is developed in Java totally as well as it consumes very less memory on the hard disk. It encompasses many functionalities like 3D pie chart statistics, possible malicious IP address detection, TCP flow graph, various coloring rules and filters that may be applied to the captured tabulated network data. It can be used for offline capture also for reading "pcap" file format. NetCap is developed in Java so it inherently contains the platform independence, but some functionalities may be applied in Windows only. The software contains a rich and easy to use Graphical User Interface (GUI) as well as a help file to guide the novice user and help the expert user to exploit its functionalities fully

Keywords

Packet Sniffer, IP address, Java, Libpcap, Jpcap, Winpcap

I. Introduction

A packet sniffer is a wiretap device that plugs into computer networks; unlike telephone circuits, computer networks are shared communication channels. Sharing means that computers can receive information that was intended for other machines (HUB) [1]. There are many packet sniffer softwares available in the market. The most popular among them is TcpDump [2] and Wireshark [3]. Though they are very good softwares for packet sniffing, there are some limitations associated with these softwares.

II. Limitations of Existing Packet Sniffer Softwares

TcpDump is very economical in terms of memory because its installation file size is just 484 KB. TcpDump does not have a user friendly Graphical User Interface (GUI). So the user has to study those commands and get acquainted with the command prompt like screen. That limitation may play a key role in not choosing it for use. On the other hand Wireshark has a very good user friendly GUI. But its installation file size is 18 MB and after installation it will consume 81 MB in Windows and a hefty 449 MB in Linux. So in terms of memory requirements, it is very expensive.

III. NetCap

We have developed NetCap which is a packet sniffer totally developed in Java^{TM}. NetCap does not have both the limitations as well as it adds some of the advantages to the packet sniffing.

A. Advantages

NetCap has a very rich and user friendly GUI developed in Java Swing Technology. Thus it is totally easy to use.With Java, the most considerable advantage is platform independence. So NetCap is also platform independent. The installation file for NetCap is only 587 KB, so it is highly economical in terms of memory use. The additional advantage of NetCap is, it detects the Denial Of Service (DOS) attack as well as ARP cache poisoning and immediately notifies the user about it. That functionality is not available in any of the available packet sniffer software. The user has to manually analyze all the packets and decide it.

B. Disadvantages

The main disadvantage of NetCap is that it is still in development stage so it is not able to identify all the protocols. Some functionalities are not available in NetCap, but due to only 2 developers working on it, it will take time to incorporate those functionalities. But it contains basic features of the packet sniffer software that are used by general user.

C. Basic Requirements

For installation on Windows it will require WinPcap software which can be downloaded from this site [4] for free.
Jpcap [5] is a set of Java classes which provide an interface and system for network packet capture. It is required for packet capture in Java. It is build upon Libpcap which is packet capture library in C language.We should have Java Runtime Environment (JRE) [6] 5.0 or higher to run this Java application.
JFreeChart [7] is another java library required for rendering 3D pie chart for captured packet statistics.

D. Installation

Only 1 MB space is required on hard disk for installation. More space may be required to store the captured packets.
First, you have to install WinPcap.
After that installation, copy the file Jpcap.dll, which will be there in Jpcap library, to C:/windows/system32 folder.

E. Features

NetCap has many salient features listed below.

- It captures the live packet information in promiscuous and non-promiscuous mode.
- NetCap shows all the network interfaces and enable to capture data from that interface.
- It also shows the statistics of the received packets.
- It can save the captured packets.
- It can retrieve the contents of the previously saved packet capture (Pcap) file.
- It can detect malicious IP addresses according to its number of ARP requests in previously specified time.
- It can also detect DOS attack and inform the user by popup.
- NetCap is able to apply coloring rules to different kind of packets and able to edit them.
- It can show the TCP flow graph generated from the received TCP packets.
- It also has a help file (.chm format) for additional required help.

F. Screenshots of NetCap

The screenshots can be enlarged by coping in another word document. They are resized to fit in the paper.

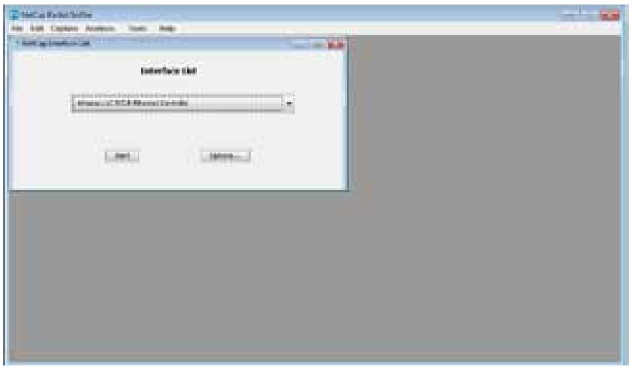

Fig. 1 : The main GUI of NetCap

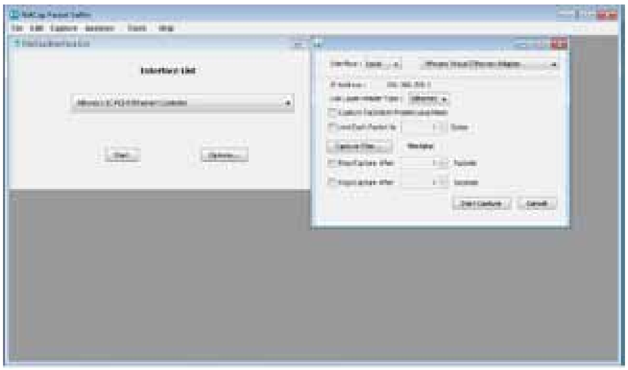

Fig.2 : After pressing the “Options” button in the “Interface List”

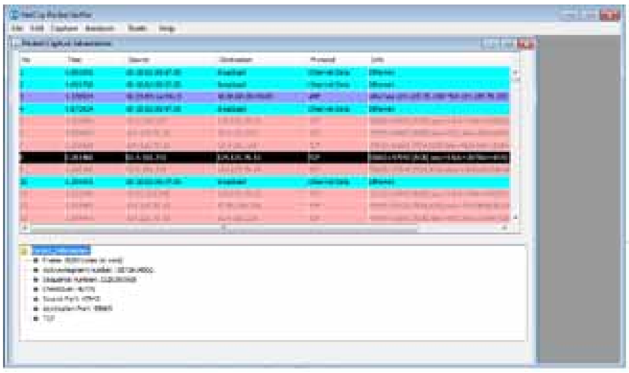

Fig.3 : The captured packets in default coloring rules per protocol

Fig. 4 : You can select saved pcap file for offline capture

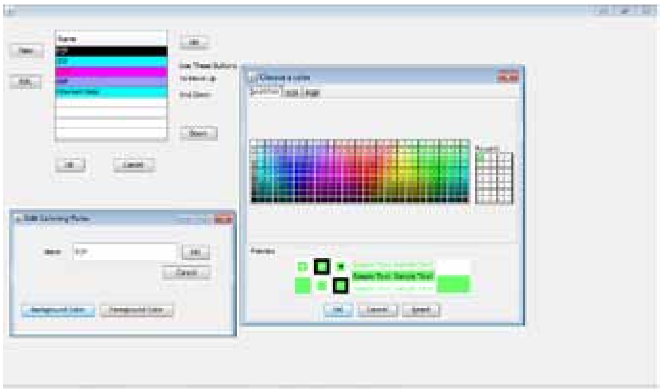

Fig. 5 : You can apply different coloring rules for every protocol.

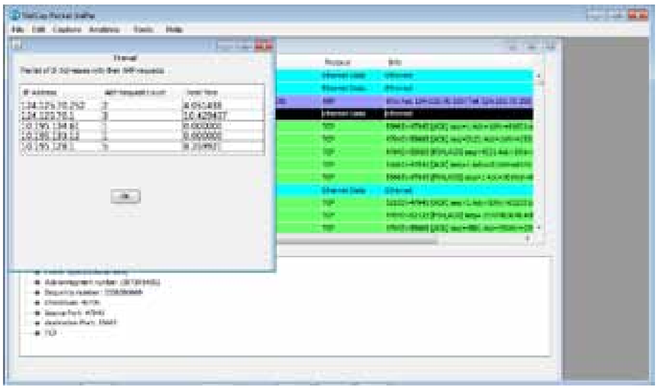

Fig. 6 : The basic firewall showing the received ARP request count in particular time.

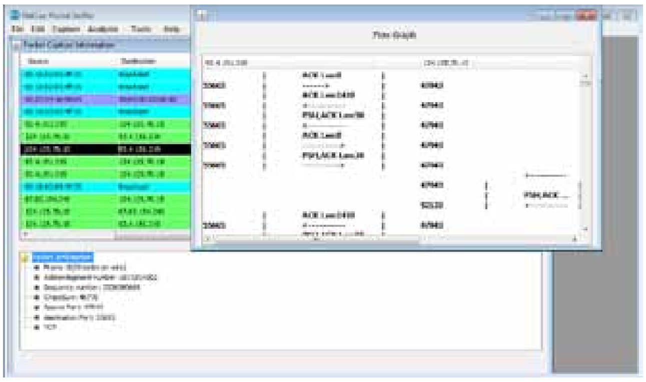

Fig. 7 : TCP Flow Graph for received packets

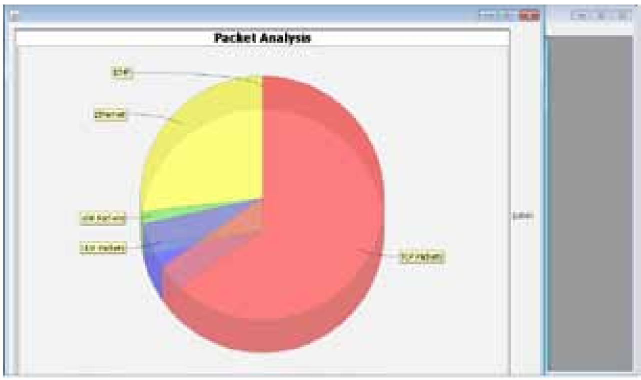

Fig. 8 : 3D pie chart showing received packet characteristics

References

[1] [Online] Available : http://www.sniffem.com/whitepaper/complete.htm

[2] All about Wireshark at [Online] Available : http://www.wireshark.org/

[3] All about TcpDump [Online] Available : http://www.tcpdump.org/

[4] Winpcap [Online] Available : http://www.wipcap.org/download

[5] Jpcap [Online] Available : http://jpcap.sourceforge.net/

[6] JRE [Online] Available : http://www.oracle.com/technetwork/java/javase/downloads/index.html

[7] JFreeChart [Online] Available : http://www.jfree.org/jfreechart/download.html

Rajan Parmar is currently working with Accenture Services Pvt. Ltd. India as an Associate Software Engineer.

Hetal Patel is currently working with Accenture Services Pvt. Ltd. India as an Associate Software Engineer.