International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 5, May - 2013

Network Army: Capture, Store & Analyze Network Traffic

Jitendra K. Karia
GTU, Gujarat Technological University

Abstract

The increased use of internet also led to increase in cyber crime activities. To enforce cyber laws, cyber crime should be proved. This led to invention of various network monitoring tools. This topic refers to developing a network monitoring tool which can capture the packets of the network on which it is placed. The tool can also work as a firewall in certain occasion. The term "network monitoring" involves the system which continuously monitors a network for slow speed or components failures. On detection of such events, it can also notify the administrator as required. The tool can also provide facility to capture only user desired protocols.

The basic operation done by network monitoring system is to monitor the network overloaded problems or servers problems like server crash, network connections or other devices. Due to this operation, NMS is able to know about the current running status of network during normal operations. Thus on the basis of result generated by NMS, we are able to identify system specific activities & its performance which helps in maintaining network requirements. Thus in order to maintain network's current health, ensuring availability along with good performance, the NMS are first to rely upon.

1. Introduction

Network monitoring & measurement have become more & more requirement for today's fast growing complicated networks. Before, administrators work was to only monitor a few n/w devices or few personal computers. The n/w bandwidth was also around 10 or 100 Mbps (Megabit per second); but, now administrators have to deal with not only high speed optical wired n/w (more than 10 Gbps) but also wireless networks. Thus need for more sophisticated n/w traffic monitoring & analysis tools. These tools maintain system stability & uptime by fixing n/w problems & avoid n/w failure by ensuring n/w strength.

On event of n/w failure, monitoring agents detect, isolate & correct problems in n/w & try to recover from failure. Generally, agent's job is to warn the administrator so that problem can be solved quickly. With the stable network, the administrator's job is to only monitor constantly if there is any threat from either inside or outside network. Another problem is overloaded n/w. If the failure is due to overload, information about n/w usage can be used to make a decision about future improvements.

There are various tools working with the n/w monitoring & analysis, like tools used by Simple n/w Management Protocol (SNMP), Windows Management Instrumentation (WMI), Sniffing, & Network flow monitoring & analysis. By knowing network traffic flow information, administrators can know n/w behaviour, such as application & network usage, utilization of n/w resources, & security vulnerabilities. In this report, we try to cover all possible n/w traffic monitoring & analysis tools in both public & commercial areas. [1]

2. Traffic flow information

In this section, we consider the characteristics of traffic flow information. We group n/w traffic monitoring & analysis tools into three categories based on data acquisition technique: n/w traffic flow information from n/w devices like NetFlow, such as "Cisco NetFlow" & by packet sniffer (Host-bed/Local traffic flow information) such as "snoop" & "tcpdump".[2]

2.1. Cisco NetFlow

Cisco System's "Cisco NetFlow" [3]: Cisco routers with netflow switching feature can generate n/w flow records & be exported in either UDP (User Datagram Protocol) or SCTP (Stream Control Transmission Protocol) packets to NetFlow collectors. NetFlow record is defined as version number, input & output interface SNMP indices, sequence number, number of bytes & packets observed in the flow, timestamps for the flow start & finish time, IP (Internet Protocol)

headers (Source & destination IP addresses, Source & destination port numbers, IP protocol, Type of Service value), the union of all TCP (Transport Control Protocol) flags observed over the life of the flow. [4]

For calculating packets & bytes per second, Flow timestamps are used. Routing info can be obtained from next hop IP address along with Border Gateway Protocol. The mechanism of TCP handshake process can be explained impliedly by union of TCP flags [5]. NetFlow 9 includes all of above information & optionally includes extra information, such as Multiprotocol Label Switching (MPLS) labels & IP version 6 addresses & port numbers [6]. Here the routers do not save flows once they are reached destination for performance reason. Due to this reason, with UDP transmission, there is no retransmission mechanism [14].

2.2. Local traffic flow information (by packet sniffer)

A "sniffer" can be of two types viz. h/w or software, whose work is to intercept & collect the local/network traffic. A sniffer records the traffic in order to provide facility to decode & analyze the traffic data into human understandable format. A sniffer captures traffic form the n/w to which it is attached i.e. it captures only local traffic. To capture all traffic, the sniffer n/w adapter will be placed in to promiscuous mode.

2.2.1. Software sniffer (snoop, tcpdump, Wireshark)

"snoop" [7] is a packet capture tool specially designed for Solaris operating system. "snoop" works with command line interface & outputs the packet in text format. The problem with "snoop" is that it does not reassemble IP fragments. "nettl/ netfmt" [8] is the packet sniffer provided by HP-UX but still in command line. "Microsoft n/w Monitor" [9] with simple graphics user interface, is the packet sniffer which is designed for Microsoft Windows. This "sniffer" runs only on Windows NT Server 4.0 or Windows Server 2003, or system having Microsoft Systems Management Server installed.

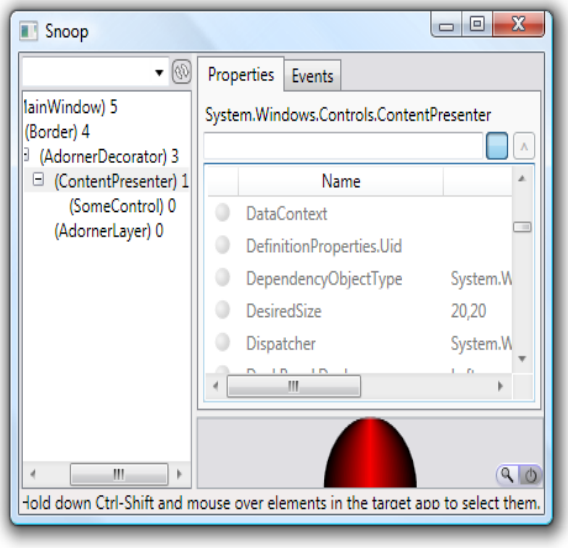

Fig 2.1: Snoop [7]

"tcpdump" [10] is a packet sniffer mainly designed for Linux operating systems, but it also supports other operating systems, such as Solaris, Mac OS X & HP-UX. "WinDump" is designed for Windows. Like "snoop", "tcpdump" runs on standard command line i.e. no GUI & outputs the captured data to text file for further analysis. In order to capture the packets in user level, "tcpdump" uses a standard libpcap library as an application programming interface.

A sniffer can analyze traffic in real-time, but this may increase processing overhead, which may result into packet drop. The solution is, first store the captured packets & do analysis later.

"Wireshark" [11], this free packet sniffer is much like "tcpdump" along with a good user-friendly interface with sorting & filtering features (a command line version is "Tshark"). "Wireshark" supports capturing packets in both from live n/w & from a saved capture file. The captured file format is stored in libpcap format like that in "tcpdump". It supports a various kinds of operating systems such as Linux, Solaris, Mac OS X, other Unix-like systems, & Windows. It can also assemble all the packets in a TCP conversation & show you the ASCII data in that conversation. Packet capturing is performed with the pcap library. Again for capturing from all n/w, permission for promiscuous mode is needed. [20]

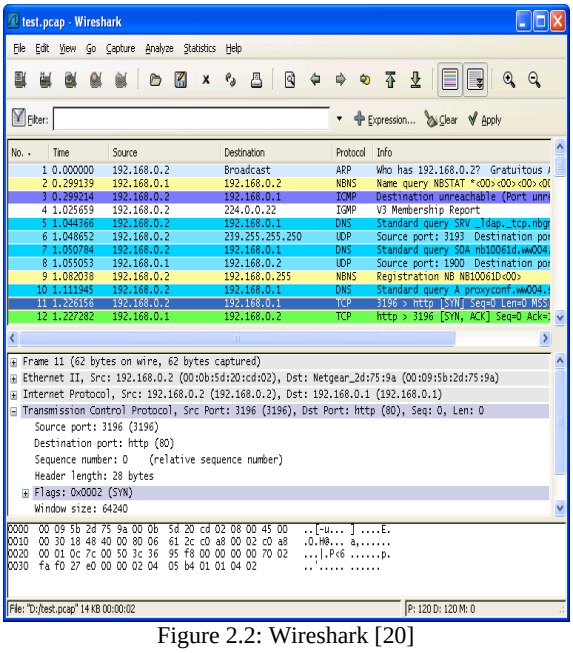

Figure 2.2: Wireshark [20]

2.2.2 Hardware sniffer (Sniffer)

There are various s/w sniffers available in market in both freeware & commercial. So what is need for h/w sniffer? The answer is, the performance of any s/w sniffer depends on operating system & h/w support capacity. Although memory can be increased but there may be bottleneck for disk I/O operations & memory bandwidth. Thus, for monitoring organizations with huge networks, h/w sniffer might be required. The h/w sniffer components such as n/w adapter, memory/disk bandwidth, & buffer management are optimized to do only n/w monitor & analysis jobs.

"Sniffer" [12] by n/w Associates, Inc. is an example of the h/w sniffer. It provides the visibility to multi-topology 10/100/1000 Ethernet, 10GbE, WAN, & ATM networks to identify, monitor, measure, & analysis of n/w problems. Again like Wireshark, "Sniffer" supports real-time analysis, back-in-time analysis, & historical analysis. The logging storage can also be supported for up to four terabytes of storage. The only thing is, Sniffer has its own memory and own unit for capturing & analyzing network data. Web-based user interface feature allow the administrator do online monitoring remotely.

3. Conclusion

As the n/w keeps growing, the need of n/w monitoring & analysis tools have been increasing. The administrator's jobs are to not only monitor an n/w failure by fix the n/w problem on time, but also avoid the n/w failure because of n/w overload or outside threat. The n/w traffic information is used to meet the administrators need. For example, n/w utilization & network traffic characteristics can detect security vulnerabilities. And, the type of application consuming bandwidth can be used for n/w planning.

A packet sniffer is a local tool where the device is attached. The information provided ny NetFlow from Cisco is very much useful, but limitation of high cost implementation for storing captured traffic remains. New sniffers can also provide with more users friendly GUI along with user defined Graph Generation technique.

Latest research may be considered more on wireless packets capturing due to the increase of wireless technology.

4. References

[1] "Traffic Monitoring using sFlow", 2003. Available: http://www.sflow.org/
[2] "NetFlow," Free encyclopedia 2006. Available: http://en.wikipedia.org/wiki/NetFlow
[3] "Cisco CNS NetFlow Collection Engine". Available: http://www.cisco.com/en/US/products/sw/netmgtsw/ps1964/index.html
[4] "NetFlow," Free encyclopedia 2006. Available: http://en.wikipedia.org/wiki/NetFlow
[5] "Cisco NetFlow site reference". Available: http://www.cisco.com/en/US/products/ps6601/products_white_paper0900aecd80406232.shtml
[6] "Internet Protocol Flow Information eXport", 2006. Available:http://www.ietf.org/html.charters/ipfixcharter.html, http://tools.ietf.org/wg/ipfix/
[7]"snoop". Available: http://docs.sun.com/app/docs/doc/816-5166/6mbb1kqh9?a=view
[8] "HOW TO TAKE A n/w TRACE ON HP-UX". Available: http://www.compute-aid.com/nettl.html
[9] "Microsoft n/w Monitor". Available: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netmon/netmon/network_monitor.asp
[10] "tcpdump". Available: http://www.tcpdump.org/
[11] "Wireshark". Available: http://www.wireshark.org/
[12] Sniffer InfiniStream. Available: http://www.networkgeneral.com/Products_details.aspx?PrdId=20046117180712
[13] Solarwinds White Paper "Geek's Guide to the NetFlow v9 Datagram".
[14] 2011 IEEE Xplore "Behavior based n/w traffic analysis tool" by Kakuru.