Comparative Study of Network Monitoring Tools

Shrutika Suri, Vandna Batra

Abstract*: There are billions of packets flying around the web sky today. A significant number of them are of malicious intent. These packets help us to understand when there are notable security or performance events occurring on the network and also to find out common network problems such as loss of connectivity, slow network etc.This paper focus on the comparative study of different packet analyzers available in current market and how we can choose amongst them according to our requirements.

Keywords: Packetcapturing, Packetanalysis, Wireshark, Eherape, capsa, libpcap.

I. INTRODUCTION

To provide a precise view on each tool we have segregated them into different categories such as console based, GUI based or both. We conducted a comprehensive review of different tools such as wireshark, tcpdump, etherape, netsniff-ng, capsa etc.

The packet capturing libraries used by these tools are libpcap,winpcap,libc etc.The languages in which these tools are developed such as C,C++,perl and the operating system they support such as linux,windows,unix and we have also discussed the pros and cons of each tool over the other which will help the user to select the packet analyzer according to their requirement[1].

II. CAPTURING LIBRARIES USED BY DIFFERENT TOOLS

1. *Wireshark* is the world's most popular network analyzer. This is a very powerful tool that provides network and upper layer protocols information about data captured in a network. It uses the pcap network library to capture packets [5].
2. *Tcpdump* is a common packet analyzer that runs under the command line. It allows the user to intercept and display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. It uses libpcap packet capturing library. WinDump is the Windows version of TCPDump. It uses the WinPcap library, which is the Windows version of libpcap [2].
3. Netsniff-ng, a zero-copy analyzer, packet capturer and replayer itself supports the pcap file format [7].
4. EtherApe is a packet sniffer/network traffic monitoring tool, developed for UNIX. EtherApe is free, open source software developed under the GNU General Public License [8].
5. Capsa is an easy-to-use portable network analyzer. It is an ideal network tool for real-time network monitoring, network analysis and troubleshooting [9].

III. OPERATING SYSTEM SUPPORT

To segregate each tool on the basis of operating system they support, will help the user to understand and use each tool according to their requirements.

- Wireshark is cross-platform, using the GTK+ widget toolkit to implement its user interface, and using pcap to capture packets; it runs on various Unix-like operating systems including Linux, Mac OS X, BSD, and Solaris, and on Microsoft Windows[1].
- Tcpdump works on most Unix-like operating systems: Linux, Solaris, BSD, Mac OS X, HP-UX and AIX among others[2].
- Netsniff-ng is a free, performant Linux networking toolkit.
- EtherApe is a graphical network monitor for Unix and Unix like operating systems [3].

IV. KEY FEATURES

Wireshark:

- ➢ Data can be captured "from the wire" from a live network connection or read from a file that recorded already-captured packets.
- ➢ Live data can be read from a number of types of network, including Ethernet, IEEE 802.11, PPP, and loopback.
- ➢ Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, TShark.
- ➢ Captured files can be programmatically edited or converted via command-line switches to the "editcap" program.
- ➢ Data display can be refined using a display filter.
- ➢ Plug-ins can be created for dissecting new protocols.
- ➢ VoIP calls in the captured traffic can be detected. If encoded in a compatible encoding, the media flow can even be played.
- ➢ Raw USB traffic can be captured.[10]

***Tcpdump*:**

It's the oldest and most commonly used network sniffer.

- ➢ It is command line-based and runs on UNIX-based systems.
- ➢ It was developed by the Network Research Group (NRG) of the Information and Computing Sciences Division (ICSD) at Lawrence Berkeley National Laboratory (LBNL) and is now being actively developed and maintained at www.tcpdump.org.
- ➢ TCPDump can be used to read live packets from the wire, or to read previously saved packet cap-tures.

Revised Manuscript Received on 30 August 2012

*****Correspondence Author(s)
Shrutika Suri*, M.Tech Student, IIIT Pune (M.H), India.
Vandna Batra, A.P MRIU, Faridabad, (U.P), India.

- It also uses a very extensive filter language. Ethereal uses this same filter language for its capture filters. When it is finished capturing data it will display the packets received and packets dropped.

The detail and length of the TCPDump output can be controlled by various options including -q, -v, -vv, -vvv, and -X. When capturing to a file, however, all of the packet detail is logged [6].

- *Netsniff-ng*: It's a zero-copy analyzer, packet capturer and replayer itself supporting the pcap file format.
- *Trafgen:* It's a zero-copy wire-rate traffic generator.
- *Bpfc:* It's a Berkeley Packet Filter compiler.
- *Ifpps***:** It's a top-like kernel networking statistics tool.
- *Flowtop*: It's is a top-like netfilter connection tracking tool.
- *Curvetun:* It's a lightweight multiuser IP tunnel based on elliptic curve cryptography
- *Ashunt:* It's an Autonomous System trace route utility.
- Capsa: Real-time capture and save data transmitted over local networks, including wired network and wireless network like 802.11a/b/g/n.
- Identify and analyse more than 300 network protocols, as well as network applications based on the protocols;
- Monitor network bandwidth and usage by capturing data packets transmitted over the network and providing summary and decoding information about these packets;
- View network statistics at a single glance, allowing easy capture and interpretation of network utilization data;
- Monitor Internet, e-mail and instant messaging traffic, helping keep employee productivity to a maximum;
- Diagnose and pinpoint network problems in seconds by detecting and locating suspicious hosts;
- Map out the details, including traffic, IP address, and MAC, of each host on the network, allowing for easy identification of each host and the traffic that passes through each;
- Visualize the entire network in an ellipse that shows the connections and traffic between each host.

V. MECHANISM

1. *Wireshark*, formerly known as Ethereal, offers a polished interface and industrial strength capabilities, plus it's as good as any packet sniffer that costs thousands of dollars.
    - Packet capture provides information about network data packets, such as the transmit time, source, destination, protocol type (TCP, IGMP or HTTP) and "header" data such as sequence and acknowledgements.
    - Wireshark will typically display information in three panels: the transmission overview, packet details and a pane showing raw hex.
    - If you need to see what is inside the packets, you're going to have to plug a host into the network somewhere along the path traversed by the packets.
    - While most network cards ignore packets not addressed to them, Wireshark places the interface it's capturing in promiscuous mode.
    - Users can also create and save filters for later use. Wireshark supports built-in searches to hone in on specific data or conditions, and will even build I/O graphs to show usage by packet type [1], [2].
2. *Tcpdump* captures packets on the network by placing a local interface in promiscuous mode.
    - Normally, your network interface will ignore any pockets that aren't addressed to your system. By placing your interface in promiscuous mode, tcpdump captures all packets, regardless of address, and allows you to examine their headers.
    - The tcpdump program also allows you to extract particular types of network traffic based on header information.
    - *Netsniff-ng* was initially created as a network sniffer with support of the Linux kernel zero-copy interface for network packets, but later on, more tools have been added to make it a useful toolkit such as the iproute2 suite, for instance.
    - The toolkit currently consists of a network analyzer, packet capturer and replayer, a wire-rate traffic generator, an encrypted multiuser IP tunnel, a Berkeley Packet Filter compiler, networking statistic tools, an autonomous system trace route and more.
3. *Etherape's* network traffic is displayed using a graphical interface. Each node represents a specific host. Links represent connections to hosts. Nodes and links are color coded to represent different protocols forming the various types of traffic on the network. Individual nodes and their connecting links grow and shrink in size with increases and decreases in network traffic. It supports Ethernet, FDDI, Token Ring, ISDN, PPP, SLIP and WLAN devices, plus several encapsulation formats. It can filter traffic to be shown, and can read packets from a file as well as live from the network [8].
4. Capsa is an easy-to-use portable network analyzer. It is an ideal network tool for real-time network monitoring, network analysis and troubleshooting. Capsa offers a comprehensive visibility of your LAN/WLAN network. The main capabilities of Capsa network analyzer include in-depth packet decoding, advanced protocol analysis, and automatic expertdiagnosis[9].

VI. CONCLUSION

The version of this template is V2. Most of the formatting instructions in this document have been compiled by Causal Productions from the IEEE LaTeX style files. Causal Productions offers both A4 templates and US Letter templates for LaTeX and Microsoft Word. The LaTeX templates depend on the official IEEEtran.cls and IEEEtran.bst files, whereas the Microsoft Word templates are self-contained. Causal Productions has used its best efforts to ensure that the templates have the same appearance.

VII. ACKNOWLEDGMENT

The heading of the Acknowledgment section and the References section must not be numbered.

Causal Productions wishes to acknowledge Michael Shell and other contributors for developing and maintaining the IEEE LaTeX style files which have been used in the preparation of this template. To see the list of contributors, please refer to the top of file IEEETran.cls in the IEEE LaTeX distribution.

REFERENCES

1. Network Traffic Monitoring ieee paper: www.ijarcsse.com/docs/papers/january2012/V2I1059.pdf by Prof. Radha S. Shirbhate
2. iresharkIntroduction: http://en.wikipedia.org/wiki/Ettercap_%28computi ng%29wireshark
3. A Survey of Network Traffic Monitoring and Analysis Tools
4. www.cse.wustl.edu/~jain/cse567-06/ftp/net...monitors3/index.htm Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection by Usha Banerjee
5. Wireshark machanisms:http://en.wikipedia.org/wiki/Wireshark
6. Tcpdump introduction: .http://en.wikipedia.org/wiki/Tcpdump
7. Netsniff-ng –the packet sniffing beast:-.http://netsniff-ng.org/
8. Etherape introduction and key features:- http://en.wikipedia.org/wiki/Etherape
9. Capsa:-.http://en.wikipedia.org/wiki/Capsa
10. WiresharkFeatures:-.http://www.wireshark.com/wireshark-reviews downloads.html
11. http://www.wireshark.org/about.html

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)