**Comparison between two packet sniffing tools: Wireshark and Tcpdump**

**Packet sniffing:-**

A packet sniffer is also called as protocol analyser is a computer program used to observe network traffic. Sniffers operate by scanning streams of data packets that go between computers connected to a network and between that network and the wider Internet. [1]

Packet sniffers are known for decoding the raw data packets flowing through a data stream. They can also store data for later use. Packet sniffers can be used on both wired and wireless networks. [1]

According to various industry and individual needs, there are hundreds of packet sniffers available on the market, some of which include WinDump, Savvius Omnipeek Wireshark, and tcpdump. But of all these,Tcpdump and Wireshark are mostly used tools. [1]

* 1. Wireshark

Wireshark is the most widely used network sniffing tool. Any type of network can be scanned with Wireshark, including Ethernet, Wi-Fi, monitor mode, and Bluetooth. In addition, it serves as an intrusion detection system (IDS). Network security breaches such as Denial of Service (DOS) assaults can be quickly identified and reported using Wireshark. [2]

Tcpdump

Tcpdump is one of the lightest network traffic capturing tool. Tcpdump is good for understanding TCP/IP as it dumps the packets in raw format without much analysis. Tcpdump offers numerous options for seeing packet details in various forms, such as the '-t' option, which produces a timestamp that can be read by humans. [3]

Comparison:

Tcpdump has the ability to dump packets only when matching strings, integers, or even a C programme are present.While Wireshark will dump every packet before applying the appropriate filter. [3]

Tcpdump uses very little battery (Zero percent), compared to Wireshark's 0.2% usage. [3]

If IPsec ESP packets are built with encryption, Tcpdump can decrypt them. In Wireshark, this function is absent.

|  |  |  |
| --- | --- | --- |
| S.NO | WIRESHARK | TCPDUMP |
| 1. | Free and open source tool | Free and open source tool |
| 2. | It can perform online and offline analysis. | It captures the packet and performs the analysis online |
| 3. | Multiplatform: Runs on Windows, Linux, OS X and so on | It supports OS like Linux, Mac OS, Solaris etc |
| 4. | It displays most powerful filters | Applying filters is difficult |
| 5. | GUI based sniffer tool | Command line tool |
| 6. | Virtual size is 620-640 Mb | Virtual size of Tcpdump is 27-29 Mb |
| 7. | Resident size of Wireshark is 87-91 Mb | RES of tcpdump is 5.8-6.3 Mb |

Conclusion:

From the above findings, Tcpdump is superior to Wireshark in terms of battery life, memory utilisation but Wireshark excels at packet analysis and capture speed.

References:

Goyal, Piyush & Goyal, Anurag. (2017). Comparative study of two most popular packet sniffing tools-Tcpdump and Wireshark. 77-81. 10.1109/CICN.2017.8319360. [1]

https://www.wireshark.org/docs/ [2]

https://www.tcpdump.org/manpages [3]