TCP Dump

Packet Analyzer that runs under the command line, allows user to display TCP/IP and other packets being transmitted or received over a network.

TCP Dumps print the content of network packets, read packets from a network interface card or saved packet file, write packets to standard output or a file.

TCP Dump can also be used for the specific purpose of intercepting and displaying communications of another user or computer.

With the necessary privileges on a system acting as a router or gateway, can view telnet or http passes to see login IDs, passwords, url and contents of websites being viewed or possibly other unencrypted information.

Users can also apply filters to limit the number of packets seen by TCP dumps, which renders the output more usable on networks with high volumes of traffic

TCP dump requires a Superuser Privilege, as features such as packet capture require elevated privilege. It is possible to allow non-privilege users to use it (alternative methods)

TCP dump has output with timestamps and study odd network latency packet by packet, import files into other tools like wireshark

Possibly cause overhead but can be overcome using socket ring buffers, or filters, but might have problems with busy interface

Limitations

* Address found maybe spoofed in the IP Packet
* Hardware -> Ethernet cards will discard packets with erroneous CRC (can’t be examined)
* Requires root privilege due to promiscuous mode