Ford’s Notes: Using tcpdump

tcpdump is a Linux network packet capture and analysis application that runs from a command line interface. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.

See: https://www.tcpdump.org/

tcpdump Commands

Display available interfaces

To get a list of available interfaces on the system you can run the following command:

tcpdump -D

Capture packets from a specific interface

If you execute the TCPdump command with the “-i” flag you can name an interface and the TCPdump tool will start capture that specific interface packets for you.

tcpdump -i eth0

Capture only specific number of packets

Using “-c” flag will allow you to capture a specific number of packets, for example, with the command below we can capture 20 packets of our eth0 interface:

tcpdump -i eth0 -c 20

Capture and save packets in a file

TCPdump has a feature to capture and save its result in a “.pcap” file, to do this just execute:

tcpdump -w eth0.pcap -i eth0

If you don’t use “-c” flag it will start capturing eth0 and write the result to the output file until you break it with “Ctrl+c”.

Note that using the -w option creates an output file that tcpdump can then read. Using the -w option is not the same as redirecting the command out to a file using ‘>’ at the command line.

Ford’s Notes: Using tcpdump

To read the file that you just created execute:

tcpdump -r eth0.pcap

Capture IP address packets

If you want to capture your network interface and analyze the IP address you can use the “-n” flag it will stop translating IP addresses into Hostnames and This can be used to avoid DNS lookups.

tcpdump -n -i eth0

Capture only TCP packets

To capture packets based on TCP ports, add a “tcp” in your command:

tcpdump -i eth0 -c 20 -w tcpanalyze.pcap tcp

Capture packets from a specific port

Let’s assume you want to monitor on a specific port like 80, you can use the following command to do that with TCPdump:

tcpdump -i eth0 port 80

Filter records with source and destination IP

To Capture packets from a source IP you can use the following command:

tcpdump -i eth0 src 192.168.1.1

You can monitor packets from a destination IP as well with the command below:

tcpdump -i eth0 dst 192.168.1.1

Notes about interfaces

Q: When using tcpdump to capture packets why do I see only packets to or from my machine, or why do I not see all the traffic from or to the machine I'm trying to monitor?

A: This might be because the interface on which you're capturing is connected to a switch. On a switched network, unicast traffic between two ports will not appear on other ports; only broadcast and multicast traffic will be sent to all ports.

Ford's Notes: Using tcpdump

Some switches can replicate all traffic on all ports to a single port (using the switch SPAN or IP EXPORT commands) so that you can plug your analyzer into that single port to sniff all traffic.

Most network interfaces can also be put in "promiscuous" mode, in which they supply to the host all network packets they see. Tcpdump will try to put the interface on which it's capturing into promiscuous mode unless the -p option was specified. However, some network interfaces don't support promiscuous mode, and some OSes might not allow interfaces to be put into promiscuous mode.

If the interface is not running in promiscuous mode, it won't see any traffic that isn't intended to be seen by your machine. It **will** see broadcast packets, and multicast packets sent to a multicast MAC address the interface is set up to receive.