TcpDump Cheat sheet

Here is the list of most popular tcpdump that Dhound team use for production network troubleshooting or capture security events.

Tcpdump is a command line network packet sniffer for Linux-based systems. Tcpdump can be installed by default in some Linux distributions (just type in command line tcpdump), overwise, install it by the command.

apt-get install tcpdump

PS. Wireshark is one of the best network sniffers for Windows-based systems.

NOTE! IP addresses specified in commands are just examples.

- track all UDP traffic initiated by host (useful to track DNS amplification attack)
  tcpdump -i any 'udp && src host 172.31.7.188' -vvnnS

- track DNS traffic that comes on the host
  tcpdump -i any '(udp && port 53 && dst host 172.31.7.188)' -vvnnS

- track TCP SYN packages from host: host tries to make to initiate TCP connection with an external source
  tcpdump -i any '((tcp[tcpflags] == tcp-syn) && src 172.31.7.188)' -vvnnS

- track TCP SYN-ACK packages to host: external resources sent acknowledge about opening TCP connection
  tcpdump -i any '(tcp[13] = 18 and dst host 172.31.7.188)' -vvnnS

- track traffic into Redis and write all packets into pcap file (pcap file can be opened in Wireshark then for analysis)
  tcpdump -i any 'dst port 6379' -vvnnS -w redis.pcap

- track all UDP output traffic except DNS
  tcpdump -i any '(udp and not dst port 53 and src host 172.31.7.188)' -vvnnS

- track all traffic with particular host with writing it into pcap file (pcap file can be opened in Wireshark then for analysis)
  tcpdump -i any 'host 172.31.7.188' -vvnnS -w host-172-31-71-88.pcap

- track all traffic on host except SSH, HTTPS, DNS, RabbitMQ, arp traffic
  tcpdump -i eth0 'not (port 22 or 443 or 53 or 5672) and not arp' -nnvvS

Usefull tcpdump parameters:

- *D* – show all interfaces
- *i* - interface
- *nn* – without resolving hostname and ports
- *vv* - verbose output
- *S* - get entire package