Tcpdump Best Practices

List of interfaces on which tcpdump can listen:

[crayon-6684cb25ce8d4108972867/]
Listen on interface eth0:
[crayon-6684cb25ce8d9025309554/]
Listen on any available interface :
[crayon-6684cb25ce8db075034266/]
Be verbose while capturing packets:
[crayon-6684cb25ce8dd698836439/]
More verbose while capturing packets:
[crayon-6684cb25ce8df978232838/]
Very verbose while capturing packets:
[crayon-6684cb25ce8e1168043844/]
Verbose and print the data of each packet in both hex and ASCII, excluding the link level header:
[crayon-6684cb25ce8e3413878718/]
Verbose and print the data of each packet in both hex and ASCII, also including the link level header:
[crayon-6684cb25ce8e5810722797/]
Less verbose (than the default) while capturing packets:
[crayon-6684cb25ce8e7614417855/]
Limit the capture to 100 packets:
[crayon-6684cb25ce8e8070189266/]
Record the packet capture to a file called capture.cap:
[crayon-6684cb25ce8ea729344335/]
Record the packet capture to a file called capture.cap but display on-screen how many packets have been captured in real-time:
[crayon-6684cb25ce8ec796068430/]
Display the packets of a file called capture.cap:
[crayon-6684cb25ce8ee002697623/]
Display the packets using maximum detail of a file called capture.cap:
[crayon-6684cb25ce8f0739769831/]
Display IP addresses and port numbers instead of domain and service names when capturing packets

[crayon-6684cb25ce8f2735510757/]
Capture any packets where the destination host is 192.168.5.1. Display IP addresses and port numbers:
[crayon-6684cb25ce8f4689522449/]
Capture any packets where the source host is 192.168.5.1. Display IP addresses and port numbers:
[crayon-6684cb25ce8f6328662498/]
Capture any packets where the source or destination host is 192.168.5.1. Display IP addresses and port numbers:
[crayon-6684cb25ce8f8202693765/]
Capture any packets where the destination network is 192.168.5.0/24. Display IP addresses and port numbers:
[crayon-6684cb25ce8fa140025640/]
Capture any packets where the source network is 192.168.1.0/24. Display IP addresses and port numbers:
[crayon-6684cb25ce8fc775411779/]
Capture any packets where the source or destination network is 192.168.5.0/24. Display IP addresses and port numbers:
[crayon-6684cb25ce8fe065011219/]
Capture any packets where the destination port is 23. Display IP addresses and port numbers:
[crayon-6684cb25ce900488338421/]
Capture any packets where the destination port is is between 1 and 1023 inclusive. Display IP addresses and port numbers:
[crayon-6684cb25ce902520805564/]
Capture only TCP packets where the destination port is is between 1 and 1023 inclusive. Display IP addresses and port numbers:
[crayon-6684cb25ce904151563965/]
Capture only UDP packets where the destination port is is between 1 and 1023 inclusive. Display IP addresses and port numbers:
[crayon-6684cb25ce905821241539/]
Capture any packets with destination IP 192.168.1.1 and destination port 23. Display IP addresses and port numbers:
[crayon-6684cb25ce908832055114/]
Capture any packets with destination IP 192.168.5.1 and destination port 80 or 443. Display IP addresses and port numbers:
[crayon-6684cb25ce90a326804680/]
Capture any ICMP packets:

[crayon-6684cb25ce90c957269989/]
Capture any ARP packets:
[crayon-6684cb25ce90d263568368/]
Capture either ICMP or ARP packets:
[crayon-6684cb25ce90f765126469/]
Capture any packets that are broadcast or multicast:
[crayon-6684cb25ce911486827486/]
Capture 500 bytes of data for each packet rather than the default of 68 bytes:
[crayon-6684cb25ce913045316949/]
Capture all bytes of data within the packet:
[crayon-6684cb25ce915363231736/]