Linux and Unix Cheat Sheet

by Anonymous (West) via cheatography.com/170121/cs/35569/

TCPDump

Links

TCPDump Advanced Filters

bpfexam

Options	Description
-e	Prints the link-level header on each dump line
-n	Prevents tcpdump from converting IP addresses to names when printing output
-nn	Prevents tcpdump from resolving TCP/UDP port numbers to service names
-v	Enables verbose output. The -vv and -vvv options provide even more information
-i	Specify the interface name or number on which tcpdump should sniff
-D	Prints all network interfaces available to tcpdump
-w	Write your captured data to a file
-r	Read input from a file
-XX	Prints the entire contents of a captured frame in both hex and ASCII

Example Scenario	Example Answer
Capture frames from eth0. Capture exactly 50 frames. Capture full frames	`tcpdump -i eth0 -e -s0 -c50 -w /tmp/o ut.pcap`
Capture all traffic to or from 1.1.1.1	`tcpdump -vnni eth0 host 1.1.1.1`
Capture all IPv4 traffic	`tcpdump -vnni eth0 ip`
Capture all traffic destined for 2.2.2.2	`tcpdump -vnni eth0 dst host 2.2.2.2`
Capture all traffic between 192.168.1-1.110 and 192.16-8.111.4 only	`tcpdump -vnni eth0 host 192.16 -8.1 1.110 and host 192.16 -8.111.4`
Capture all traffic between 192.168.1-1.110 and the 192.16-8.111.0/24 network only	`tcpdump -vnni eth0 host 192.16 -8.1 1.110 and net 192.16 8.1 -11.0/24`

TCPDump (cont)

Suppose we have a tcpdump version that only allows the older syntax, and we wish to capture only traffic to the 192.168.1-5.64/26 network	`tcpdump -nnvi eth0 'ip dst net 192.168.15 and ip[19] & 0xC0 = 64'`

Ping

Options	Description
-c	Specifies the number of attempts the ping command should make to contact the remote host
-s	Specifies the number of data bytes to send in each ping attempt