

NETCAP Cheatsheet

Documentation: docs.netcap.io

Command	Description
<code>net capture -iface eth0</code>	Read traffic live from interface, stop with <i>Ctrl-C</i> (<i>SIGINT</i>)
<code>net capture -readead traffic.pcap</code>	Read traffic from a dump file (supports PCAP or PCAPNG)
<code>net capture -iface en0 -bpf "host 192.168.1.1"</code>	apply a BPF when capturing traffic live
<code>net capture -read traffic.pcap -bpf "host 192.168.1.1"</code>	apply a BPF when parsing a dumpfile
<code>net capture -read traffic.pcap -include Ethernet,Dot1Q,IPv4,IPv6,TCP,UDP,DNS</code>	Include specific encoders (only those named will be used)
<code>net capture -read traffic.pcap -exclude TCP,UDP</code>	Exclude encoders (this will prevent decoding of layers encapsulated by the excluded ones)
<code>net capture -workers 24 -buf false -comp false -read traffic.pcapng</code>	Run with 24 workers and disable gzip compression and buffering
<code>net capture -read traffic.pcap -out traffic_ncap</code>	Parse pcap and write all data to output directory (will be created if it does not exist)
<code>net dump -read TCP.ncap.gz</code>	Read a netcap dumpfile and print to stdout as CSV
<code>net dump -fields -read TCP.ncap.gz</code>	Show the available fields for a specific Netcap dump file
<code>net dump -read TCP.ncap.gz -select Timestamp,SrcPort,DstPort</code>	Print only selected fields and output as CSV
<code>net dump -read TCP.ncap.gz -select Timestamp,SrcPort,DstPort > tcp.csv</code>	Save CSV output to file
<code>net dump -read TPC.ncap.gz -tsv</code>	Print output separated with tabs
<code>net dump -read TCP.ncap.gz -select Timestamp,SrcPort,Dstport -utc</code>	Convert timestamps to UTC
<code>net dump -read TCP.ncap.gz -header</code>	Show audit record header
<code>net dump -read TCP.ncap.gz -struc</code>	Print structured audit records
<code>net dump -read TCP.ncap.gz -tsv</code>	Print audit records as Tab Separated Values
<code>net dump -read UDP.ncap.gz -table</code>	Print as table
<code>net dump -read TCP.ncap.gz -sep ";"</code>	Print audit records with Custom Separator
<code>net dump -read TCP.ncap.gz -check</code>	Check if generated output contains the correct number of separator symbols
<code>net dump -read UDP.ncap.gz -fields</code>	Show available fields for the audit record type
<code>net collect -gen-keypair</code>	generate keypair for distributed collection and write to disk
<code>net collect -privkey priv.key -addr 127.0.0.1:4200</code>	start collection server
<code>net agent -pubkey pub.key -addr 127.0.0.1:4200</code>	start a sensor agent for exporting data