tcpdump

Abstract

> *Tcpdump prints out a description of the contents of packets on a network interface that match the boolean expression; the description is preceded by a time stamp, printed, by default, as hours, minutes, seconds, and fractions of a second since midnight. It can also be run with the -w flag, which causes it to save the packet data to a file for later analysis, and/or with the -r flag, which causes it to read from a saved packet file rather than to read packets from a network interface. It can also be run with the -V flag, which causes it to read a list of saved packet files. In all cases, only packets that match expression will be processed by tcpdump.*

Source: tcpdump man page

```
$ man tcpdump
```

Where to Acquire

Available by default in many Linux distributions. For direct downloads and additional information see www.tcpdump.org

Windump is the Windows-based implementation of tcpdump that leverages the WinPcap driver. Windump and WinPcap are available from www.winpcap.org

Examples/Use Case

Note: Some of the examples below presume files and paths that might not match your particular system and tool installation.

Read a pcap file:

```
$ tcpdump -r /pcaps/zeus-gameover-loader.pcap
```

Read a pcap, don't resolve names (layers 3 or 4):

```
$ tcpdump -nr /pcaps/zeus-gameover-loader.pcap
```

Read a pcap, show TCP SYN packets, don't resolve names:

```
$ tcpdump -r /pcaps/zeus-gameover-loader.pcap -n "tcp[tcpflags]==tcp-syn"
```

Read a pcap, show TCP SYN packets not sent to port 80, don't resolve names:

```
$ tcpdump -r /pcaps/zeus-gameover-loader.pcap -n "tcp[tcpflags]==tcp-syn and not tcp dst port 80"
```

Read a pcap without name resolution, /pcaps/angler-java.pcap, and show traffic with the ACK FIN and PUSH flags set.

```
$ tcpdump -r /pcaps/angler-java.pcap -n "tcp[tcpflags]==(tcp-ack|tcp-fin|tcp-push)"
```

Additional Info

tcpdump allows the use of BPF (Berkely Packet Filter) expressions. See the pcap-filter man page for additional details on bpf filters.

```
$ man pcap-filter
```

A printable PDF version of this cheatsheet is available here:
tcpdump

Cheat Sheet Version

Version 1.0