Tcpdump Basics

Overview

What is tcpdump?

#The following is from the tcpdump man page
man tcpdump

SYNOPSIS

tcpdump [-adeflnNOpqRStuvxX] [-c count]
[-C file_size] [-F file]
[-i interface] [-m module] [-r file]
[-s snaplen] [-T type] [-w file]
[-E algo:secret] [expression]

DESCRIPTION

Tcpdump prints out the headers of packets on a network interface that match the boolean expression.

What is it typically used for?

Tcpdump is typically used for troubleshooting network applications.
It can also be used for security related purposes.

What do I need to use tcpdump and where can I get it?

libpcap (packet capture library) and tcpdump sources at http://www.tcpdump.org/

Running tcpdump

First you must determine network interface that will be monitored.

ifconfig –a
eth0 Link encap:Ethernet HWaddr 00:03:47:98:78:0A
inet addr:192.168.0.1 Bcast: 192.168.0.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:20130985 errors:0 dropped:0 overruns:0 frame:0
TX packets:2140879 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:2469919130 (2355.4 Mb) TX bytes:267848744 (255.4 Mb)
Interrupt:17 Memory:fe000000-fe020000

Then run the tcpdump command with the –i option to tell it which interface to listen on.

tcpdump –i eth0
tcpdump: listening on eth0

Common command line options

Tcpdump takes many command line options. Below are listed the more common options that are used.

#Except from the tcpdump manpage

-i Listen on *interface*. If unspecified, *tcpdump* searches the system interface list for the lowest numbered, configured up interface (excluding loop back). Ties are broken by choosing the earliest match.
On Linux systems with 2.2 or later kernels, an *interface* argument of ``any'' can be used to cap ture packets from all interfaces. Note that cap tures on the ``any'' device will not be done in promiscuous mode.

-l Make stdout line buffered. Useful if you want to see the data while capturing it. E.g., ``tcpdump -l | tee dat'' or ``tcpdump -l > dat & tail -f dat''.

-p *Don't* put the interface into promiscuous mode. Note that the interface might be in promiscuous mode for some other reason; hence, `-p' cannot be used as an abbreviation for `ether host {local-hw-addr} or ether broadcast'.

-t *Don't* print a timestamp on each dump line.

-ttt Print a delta (in micro-seconds) between current and previous line on each dump line.

-c Exit after receiving *count* packets.

-w Write the raw packets to *file* rather than parsing and printing them out. They can later be printed with the -r option. Standard output is used if *file* is ``-''

-r Read packets from *file* (which was created with the -w option). Standard input is used if *file* is ``-''.

-q Quick (quiet?) output. Print less protocol infor mation so output lines are shorter.

-v (Slightly more) verbose output. For example, the time to live and type of service information in an IP packet is printed.

-vv Even more verbose output. For example, additional fields are printed from NFS reply packets.

Basic Expressions

An expression will decide what will be dumped based on truth.
There are three different kinds of qualifiers

type
dir
proto

Some commonly used primitives

host *host*
net network
ip broadcast
ip proto *protocol*
tcp, udp, icmp
Abbreviations for:
ip proto *p*

Basic Examples

These are some examples of tcpdump's use in troubleshooting several issues.

Pings from the jclinux box to the laptop are not receiving replies.

```
# ifconfig -a
# tcpdump –pqtli eth0 host 192.168.0.1 and icmp
```

SSH from the laptop to the jclinux box are not working

```
# tcpdump –pvti eth0 –w  ./lab.cap host 192.168.0.1 and port 22
# tcpdump –r ./lab.cap
```

References

Tcpdump.1. Tcpdump.org. 20 May 2004 < http://www.tcpdump.org/tcpdump_man.html>
Stevens, Richard W. *TCP/IP Illustrated, Volume 1*. Boston: Addison-Wesley, 1994.

Further reading

http://www.faqs.org/rfcs/rfc791.html
http://www.faqs.org/rfcs/rfc793.html
http://www.ethereal.com/introduction.html