Network analysis !

Πίνακας περιεχομένων

1. Install swarmlab-sec (Home PC)

HowTo: See http://docs.swarmlab.io/lab/sec/sec.adoc.html

NOTE

Assuming you're already logged in

tcpdump is a common packet analyzer that runs under the command line. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Distributed under the BSD license, tcpdump is free software.

More: wikipedia

2. Basic

2.1. Everything on an interface

Just see what's going on, by looking at what's hitting your interface.

```
tcpdump -i eth0
```

2.2. Find Traffic by IP

One of the most common queries, using host, you can see traffic that's going to or from 1.1.1.1.

```
tcpdump host 1.1.1.1
```

2.3. Filtering by Source and/or Destination

If you only want to see traffic in one direction or the other, you can use src and dst.

```
tcpdump src 1.1.1.1
tcpdump dst 1.0.0.1
```

2.4. Finding Packets by Network

To find packets going to or from a particular network or subnet, use the net option.

```
tcpdump net 1.2.3.0/24
```

2.5. Show Traffic Related to a Specific Port

You can find specific port traffic by using the port option followed by the port number.

```
tcpdump port 3389
tcpdump src port 1025
```

2.6. Show Traffic of One Protocol

If you're looking for one particular kind of traffic, you can use tcp, udp, icmp, and many others as well.

```
tcpdump icmp
```

2.7. Reading / Writing Captures to a File (pcap)

It's often useful to save packet captures into a file for analysis in the future. These files are known as PCAP (PEE-cap) files, and they can be processed by hundreds of different applications, including network analyzers, intrusion detection systems, and of course by tcpdump itself. Here we're writing to a file called capture_file using the -w switch.

```
tcpdump port 80 -w capture_file
```

3. Advanced

Now that we've seen what we can do with the basics through some examples, let's look at some more advanced stuff.

More options

```
  -X         : Show the packet□s contents in both hex and ASCII.
  -XX        : Same as -X, but also shows the ethernet header.
  -D         : Show the list of available interfaces
  -l         : Line-readable output (for viewing as you save, or sending to other
commands)
  -q         : Be less verbose (more quiet) with your output.
  -t         : Give human-readable timestamp output.
  -tttt      : Give maximally human-readable timestamp output.
  -i eth0    : Listen on the eth0 interface.
  -vv        : Verbose output (more v□s gives more output).
  -c         : Only get x number of packets and then stop.
  -s         : Define the snaplength (size) of the capture in bytes. Use -s0 to get
everything, unless you are intentionally capturing less.
  -S         : Print absolute sequence numbers.
  -e         : Get the ethernet header as well.
  -q         : Show less protocol information.
  -E         : Decrypt IPSEC traffic by providing an encryption key.
```

It's All About the Combinations

Being able to do these various things individually is powerful, but the real magic of tcpdump comes from the ability to combine options in creative ways in order to isolate exactly what you're looking for. There are three ways to do combinations, and if you've studied programming at all they'll be pretty familiar to you.

- AND

```
and or &&
```

- OR

```
or or ||
```

- EXCEPT

```
not or !
```

3.1. From specific IP and destined for a specific Port

Let's find all traffic from 10.5.2.3 going to any host on port 3389.

```
tcpdump -nnvvS src 10.5.2.3 and dst port 3389
```

3.2. From One Network to Another

Let's look for all traffic coming from 192.168.x.x and going to the 10.x or 172.16.x.x networks, and we're showing hex output with no hostname resolution and one level of extra verbosity.

```
tcpdump -nvX src net 192.168.0.0/16 and dst net 10.0.0.0/8 or 172.16.0.0/16
```

3.3. Isolate TCP Flags

You can also use filters to isolate packets with specific TCP flags set.

3.3.1. Isolate TCP RST flags.

The filters below find these various packets because tcp[13] looks at offset 13 in the TCP header, the number represents the location within the byte, and the !=0 means that the flag in question is set to 1, i.e. it's on.

```
tcpdump 'tcp[13] & 4!=0'
tcpdump 'tcp[tcpflags] == tcp-rst'
```

3.3.2. Isolate TCP SYN flags.

```
tcpdump 'tcp[13] & 2!=0'
tcpdump 'tcp[tcpflags] == tcp-syn'
```

3.3.3. Isolate packets that have both the SYN and ACK flags set.

```
tcpdump 'tcp[13]=18'
```

Only the PSH, RST, SYN, and FIN flags are displayed in tcpdump‘s flag field output. URGs and ACKs are displayed, but they are shown elsewhere in the output rather than in the flags field.

3.3.4. Isolate TCP URG flags.

```
tcpdump 'tcp[13] & 32!=0'
tcpdump 'tcp[tcpflags] == tcp-urg'
```

3.3.5. Isolate TCP ACK flags.

```
tcpdump 'tcp[13] & 16!=0'
tcpdump 'tcp[tcpflags] == tcp-ack'
```

3.3.6. Isolate TCP PSH flags.

```
tcpdump 'tcp[13] & 8!=0'
tcpdump 'tcp[tcpflags] == tcp-psh'
```

3.3.7. Isolate TCP FIN flags.

```
tcpdump 'tcp[13] & 1!=0'
tcpdump 'tcp[tcpflags] == tcp-fin'
```

3.4. Find Traffic With Evil Bit

There’s a bit in the IP header that never gets set by legitimate applications, which we call the “Evil

Bit". Here's a fun filter to find packets where it's been toggled.

```
tcpdump 'ip[6] & 128 != 0'
```

3.5. Summary

Here are the takeaways.

- **tcpdump** is a valuable tool for anyone looking to get into networking or **information security**.
- The raw way it interfaces with traffic, combined with the precision it offers in inspecting packets make **it the best possible tool** for learning TCP/IP.
- Protocol Analyzers like **Wireshark** are great, but if you want to truly master **packet-fu**, you must become one with tcpdump

Appendix A: How to use tcpdump

This exercise will show you how to isolate traffic in various ways—from IP, to port, to protocol, to application-layer traffic—to make sure you find exactly what you need as quickly as possible.

Origin

Reminder

Caminante, no hay camino,
se hace camino al andar.

Wanderer, there is no path,
the path is made by walking.

Antonio Machado Campos de Castilla