6.5 名称解析

类似 Wireshark，TShark 和 Tcpdump 也会尝试名称解析，即把地址和端口号转换为名称。如果你注意之前的例子，也许已经发现这一过程已默默地发生了。就像之前提到的，我通常会把它关掉来避免产生更多网络流量的可能。

你可以通过-n 参数来禁用 TShark 的名称解析。这个参数可以和其他参数一起使用来增强可读性。

```
C:\Program Files\Wireshark>tshark –ni 1
```

你可以通过-N 参数来启用或禁用一些名称解析的特定功能。如果使用-N 参数，则所有的名称解析功能将会被禁用，除非你明确指定一些功能的启用。举例来说，下面的命令仅会启用传输层（端口服务名称）的解析。

```
C:\Program Files\Wireshark>tshark –i 1 –Nt
```

你可以结合多个值，下面这个命令会启用传输层和 MAC 层的解析。

```
C:\Program Files\Wireshark>tshark –i 1 -Ntm
```

当使用该选项时可能参考以下值。

m：MAC 地址解析。

n：网络地址解析。

t：传输层（端口服务名称）解析。

N：使用外网解析服务。

C：使用当前 DNS 解析。

在 Tcpdump 下，使用-n 会禁用 IP 名称解析，使用-nn 也会禁用端口服务解析。

这个参数也可以和其他命令相结合使用，就像这样：

```
sanders@ppa:~$ tcpdump –nni eth1
```

下面的例子展示了一个捕获的数据包先启用端口解析，然后再禁用（-n）。

```
   sanders@ppa:~$ tcpdump -r tcp_ports.pcap -c1
reading from file tcp_ports.pcap, link-type EN10MB (Ethernet)
14:38:34.341715 IP 172.16.16.128.2826 > 212.58.226.142.❶http: Flags
3691127924, win 8192, options [mss 1460,nop,wscale 2,nop,nop,sackOK
sanders@ppa:~$ tcpdump -nr tcp_ports.pcap -c1
reading from file tcp_ports.pcap, link-type EN10MB (Ethernet)
14:38:34.341715 IP 172.16.16.128.2826 > 212.58.226.142.❷80: Flags |
3691127924, win 8192, options [mss 1460,nop,wscale 2,nop,nop,sackOK
```

这些命令仅从捕获文件 tcp_ports.pcap 中读取了第一个包。在第一个命令里，80 端口被解析为 http。但在第二个命令，端口仅以数字形式表示。