Analyze Network Traffic with TCPDump

Project Description

The goal of this project is to create a script to monitor traffic to a particular website and analyze traffic going between it and my workstation.

Software and Utilities used

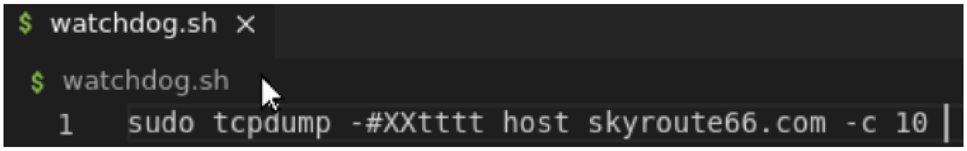
TCPDump

Cloud Workspace

Visual Studio Code

Analysis walk-through:

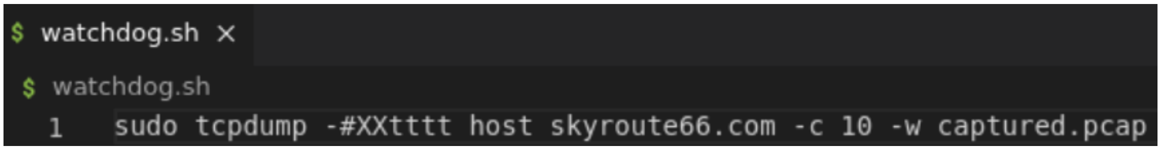
1. Create shell script



```
sudo tcpdump -#XXtttt host skyroute66.com -c 10
```

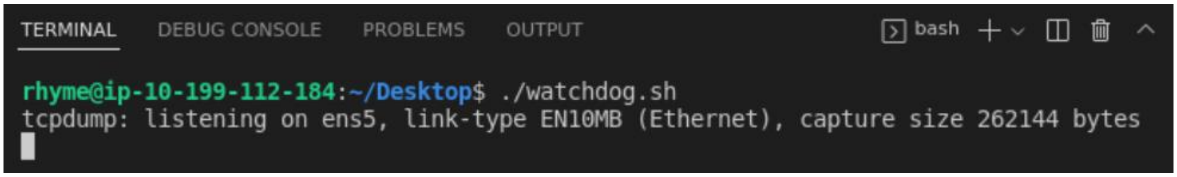
To create a shell script, I used Visual Studio Code. To capture packets for troubleshooting or analysis, tcpdump requires elevated permissions, so most commands are prefixed with `sudo`. The `-#` sign will print an optional packet number at the beginning of the line. `XX` will display the packets content in hex format. `tttt` will print a timestamp, as hours, minutes, seconds, and fractions of a second on each dump line. `host` will monitor both source and destination of traffic from the `skyroute66.com` website. The `–c` option will exit capturing after receiving count packets. In the above example, it will only capture ten packets.

2. Create and read dump files



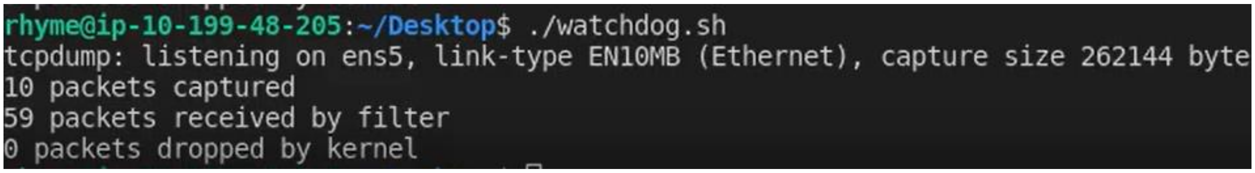
```
sudo tcpdump -#XXtttt host skyroute66.com -c 10 -w captured.pcap
```

To create a dump file, I used the -w option which writes the raw packets to the captured.pcap dump file.



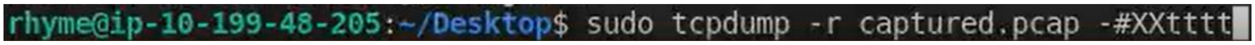
```
rhyme@ip-10-199-112-184:~/Desktop$ ./watchdog.sh
tcpdump: listening on ens5, link-type EN10MB (Ethernet), capture size 262144 bytes
```

On the integrated terminal, I attempted to execute the shell file, but it was not returning any packets. To capture packets, I proceeded to refresh the skyroute66.com website on the Cloud Workspace.



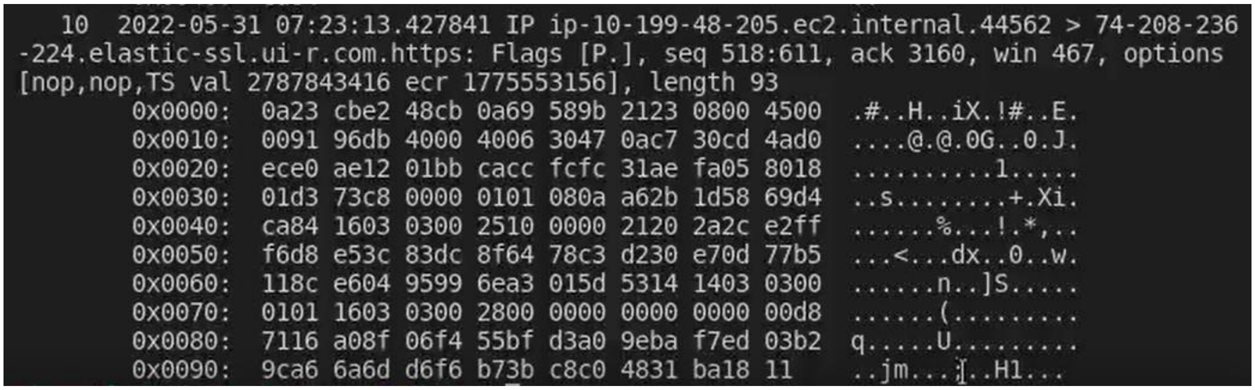
```
rhyme@ip-10-199-48-205:~/Desktop$ ./watchdog.sh
tcpdump: listening on ens5, link-type EN10MB (Ethernet), capture size 262144 byte
10 packets captured
59 packets received by filter
0 packets dropped by kernel
```

After refreshing the website, we can see that it stopped listening to traffic after capturing ten packets. Next, I proceeded to read the file by entering the following command:



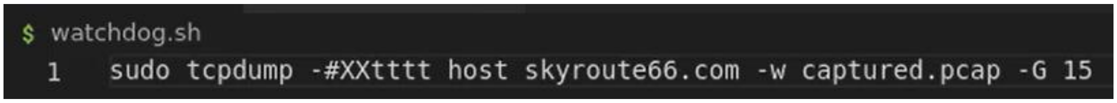
```
rhyme@ip-10-199-48-205:~/Desktop$ sudo tcpdump -r captured.pcap -#XXtttt
```

The -r option means to read the file. After reading it, the following image shows ten captured packets with a timestamp and in hex format.



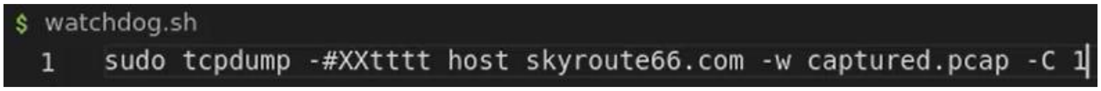
```
   10  2022-05-31 07:23:13.427841 IP ip-10-199-48-205.ec2.internal.44562 > 74-208-236
-224.elastic-ssl.ui-r.com.https: Flags [P.], seq 518:611, ack 3160, win 467, options
[nop,nop,TS val 2787843416 ecr 1775553156], length 93
        0x0000:  0a23 cbe2 48cb 0a69 589b 2123 0800 4500  .#..H..iX.!#..E.
        0x0010:  0091 96db 4000 4006 3047 0ac7 30cd 4ad0  ....@.@.0G..0.J.
        0x0020:  ece0 ae12 01bb cacc fcfc 31ae fa05 8018  ..........1.....
        0x0030:  01d3 73c8 0000 0101 080a a62b 1d58 69d4  ..s........+.Xi.
        0x0040:  ca84 1603 0300 2510 0000 2120 2a2c e2ff  ......%...!.*,..
        0x0050:  f6d8 e53c 83dc 8f64 78c3 d230 e70d 77b5  ...<...dx..0..w.
        0x0060:  118c e604 9599 6ea3 015d 5314 1403 0300  ......n..]S.....
        0x0070:  0101 1603 0300 2800 0000 0000 0000 00d8  ......(.........
        0x0080:  7116 a08f 06f4 55bf d3a0 9eba f7ed 03b2  q.....U.........
        0x0090:  9ca6 6a6d d6f6 b73b c8c0 4831 ba18 11    ..jm...;..H1...
```

3. Create a sequence of dump files with size and time limits



```
sudo tcpdump -#XXtttt host skyroute66.com -w captured.pcap -G 15
```

In the above picture, the -G option means to rotate the dump file indicated by the number of seconds. In this example, it is set to 15 seconds. After 15 seconds, it will wipe out the contents of the file and start over.



```
sudo tcpdump -#XXtttt host skyroute66.com -w captured.pcap -C 1
```

In the above picture, the -C option indicates file size. It will measure file size by million bytes, and it will not capture packets bigger than the desired size. In this example, the file size is set to one million bytes.