Ethical Hacking: Capture Report

Jordi Nadeu Ferran

Abstract

In this laboratory, we practice how to use Wireshark like an attacker capturing and analysing network packets. Mainly divided into the use of Wireshark from the Kali machine and also the tcpdump tool from the pfSense machine (router).

1 Introduction

Wireshark is a widely-used, open-source network protocol analyzer that allows users to capture, inspect, and analyze network traffic in real-time. It provides deep visibility into network packets, making it an essential tool for troubleshooting, performance analysis, and security monitoring.

tcpdump is a powerful command-line tool for capturing and analyzing network traffic. It is widely used by network administrators and security professionals to monitor network activity.

They really complement each other. On the one hand tcpdump is lightweight, fast, and effective for basic real-time network monitoring and capture, on the other hand we have Wireshark is more powerful for detailed traffic analysis and visualization. Normally the tcpdump tool often is used for capturing data and Wireshark is used for detailed inspection of that data.

In further illustrating the differences between the two tools, a table of the main differences is provided below. As shown in the figure 1.

Aspect	tcpdump	Wireshark
User Interface	Command-line tool	Graphical user interface (GUI)
Ease of Use	Requires knowledge of command-line and filters	More user-friendly, with point-and-click filtering
Output Format	Text-based packet summaries	Rich, detailed packet dissection with GUI visualizations
Protocol Analysis	Provides header-level details	Offers deep inspection of packet contents (protocols, fields, etc.)
Filtering	Uses BPF (Berkeley Packet Filter) for capturing filters	Can apply filters both before capturing (BPF) and after capture (display filters)
Decryption	Does not natively support decryption of encrypted traffic	Can decrypt traffic such as SSL/TLS (with keys)
Real-Time Capture	Displays packets in real-time in terminal	Also supports live capture, but better suited for post-capture analysis
Resource Usage	Low resource usage, suitable for headless servers	Higher resource usage due to GUI and advanced features
Packet Analysis Depth	Basic analysis (mostly header-level details)	Detailed packet analysis, including payload interpretation
Cross-Platform	Mostly available on Unix-like systems	Available on Windows, macOS, Linux

Figure 1: Main Differences Between tcpdump and Wireshark

2 Procedure

This practice starts by installing and preparing all the necessary environment to run Wireshark. As we are using the Kali distribution with a simple command we have this step done. Concretely with the following command:

```
sudo apt install wireshark
```

Once installed, we can open as root and start monitoring traffic on the 'eth0' interface.

Below is a screenshot (figure 2) of what the Wireshark application looks like with an active filter to only view TCP packets, after a connection to a web page.

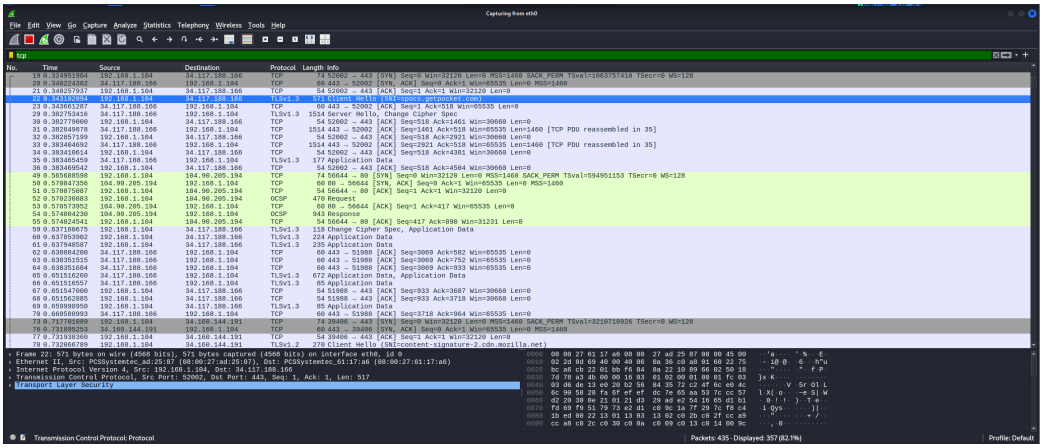

Figure 2: Wireshark TCP filter

To filter and only view TCP packets on port 443, which is typically used for HTTPS traffic, go to the display filter bar at the top and type the following: *'tcp.port == 443'*.

To do the same as in Wireshark from the Pfsense machine using the tcpdump tool, run the following command in the terminal:

```
tcpdump -i em1 tcp port 443
```

In our particular case the interface name em1 is equivalent to eth0 of the Kali machine.
The following screenshot shows what the above tcpdump command looks like.

```
15:51:09.689737 IP 192.168.1.104.40342 > 209.100.149.34.bc.googleusercontent.com
.https: Flags [.], ack 45784, win 54020, length 0
15:51:09.690409 IP 209.100.149.34.bc.googleusercontent.com.https > 192.168.1.104
.40342: Flags [.], seq 45784:47244, ack 1340, win 65535, length 1460
15:51:09.690427 IP 209.100.149.34.bc.googleusercontent.com.https > 192.168.1.104
.40342: Flags [.], seq 47244:48704, ack 1340, win 65535, length 1460
15:51:09.690471 IP 209.100.149.34.bc.googleusercontent.com.https > 192.168.1.104
.40342: Flags [P.], seq 48704:49984, ack 1340, win 65535, length 1280
15:51:09.690618 IP 192.168.1.104.40342 > 209.100.149.34.bc.googleusercontent.com
.https: Flags [.], ack 49984, win 62780, length 0
15:51:09.691364 IP 209.100.149.34.bc.googleusercontent.com.https > 192.168.1.104
.40342: Flags [.], seq 49984:51444, ack 1340, win 65535, length 1460
15:51:09.691391 IP 209.100.149.34.bc.googleusercontent.com.https > 192.168.1.104
.40342: Flags [.], seq 51444:52904, ack 1340, win 65535, length 1460
15:51:09.691407 IP 209.100.149.34.bc.googleusercontent.com.https > 192.168.1.104
.40342: Flags [P.], seq 52904:54184, ack 1340, win 65535, length 1280
15:51:09.691578 IP 192.168.1.104.40342 > 209.100.149.34.bc.googleusercontent.com
.https: Flags [.], ack 54184, win 65535, length 0
15:51:09.692170 IP 209.100.149.34.bc.googleusercontent.com.https > 192.168.1.104
.40342: Flags [P.], seq 54184:54336, ack 1340, win 65535, length 152
15:51:09.692533 IP 192.168.1.104.40342 > 209.100.149.34.bc.googleusercontent.com
.https: Flags [P.], seq 1340:1379, ack 54336, win 65535, length 39
15:51:09.692845 IP 209.100.149.34.bc.googleusercontent.com.https > 192.168.1.104
.40342: Flags [.], ack 1379, win 65535, length 0
```

Figure 3: tcpdump output

As you can see in the case of wireshark it shows more information than in the case of tcpdump command. In order to answer the questions in this exercise, we opened the pcap file with Wireshark and then applied a filter to show only ARP packets, as shown in the figure below.

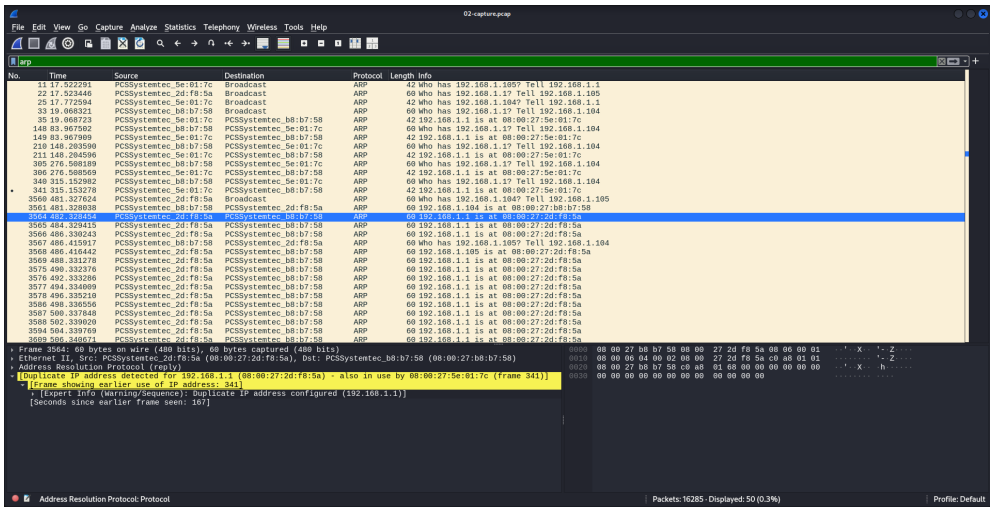

Figure 4: Wireshark capture file with ARP filter applied

Once we have carefully observed the ARP packet traffic, we can see that at the beginning of the first broadcast that the router makes, it has the IP (192.168.1.1) and the MAC (08:00:27:5e:01:7c). Then later, specifically frame 3560, which is shown in the previous screenshot, there is another broadcast and from there the victim's ARP table is poisoned, which has IP (192.168.1.104) and MAC (08:00:27:b8:b7:58). Then the attacker can see the victim's traffic, as the router IP has the attacker's MAC associated in victim ARP table.

Then the attacker IP is (192.168.1.105) with MAC (08:00:27:2d:f8:5a). In frame 3564 can see 192.168.1.1 (router IP) is at 08:00:27:2d:f8:5a (attacker's MAC).

3 Conclusions

In this practice we have learnt how to use the Wireshark tool at a basic level in order to monitor and analyse the traffic generated in a network.

Specifically, we have analysed an already prepared wireshark file in which we have found an ARP spoofing attack. As well as detecting the IP and MAC of the victim and also of the attacker.