Selachii (50)

Description

https://drive.google.com/open?id=0B_96Z9gRHRIxMkhHaDZTdUFRelU

Hint: TripleDES

Write Up

Let's analyze the PCAP file with Wireshark:

First let's filter `http`, we will see a lot of packets. What if we narrow the search to only POST to see if any private information is transferred over HTTP POST, filter by `http and http.request.method == "POST"`.

We will see that there are only 4 packet, all of them from `pastebin.xyz`. We can see from the form body:

> Form item: "code" = "Here's the key: wiresharkftw"

and

> Form item: "code" = "ksXCm1/ipkqF1TjV9YbN67z+C8pxgdhpZYNEUUqiVdg="

Then we can decode the TripleDES encrypted string with the key `wiresharkftw` to get the flag: `COMPFEST9{des_des_des_tripledes}`