Collaborative Challenge 1

David Salgado

Objective: The security team was alerted to suspicious network activity from a production web server. Can you determine if any data was stolen and what it was?

Process:

Look at the traffic and see what is suspicious. By observing the tab of statistics and conversations, when organizing by packets length I got this:

chalcap.pcapng

Ethernet · 4 | IPv4 · 105 | IPv6 · 1 | TCP · 227

Address A	Address B	Packets	Bytes
10.10.100.43	173.194.31.248	2,320	13 MB
10.10.100.43	151.101.116.193	1,712	8 MB
10.10.100.43	74.125.155.234	930	5 MB
10.10.100.43	10.10.20.1	838	99 kB
10.10.100.43	172.217.12.194	501	160 kB
10.10.100.43	23.207.174.113	478	141 kB
10.10.99.42	10.10.20.13	431	35 kB
10.10.100.43	192.33.31.52	406	106 kB
10.10.100.43	10.10.99.42	367	139 kB
10.10.100.43	172.217.10.142	346	307 kB
10.10.100.43	172.217.10.238	292	187 kB
10.10.100.43	172.217.7.14	284	126 kB
10.10.100.43	104.16.27.235	177	35 kB
10.10.100.43	173.241.242.220	162	61 kB
10.10.100.43	172.217.10.230	149	54 kB
10.10.100.43	172.217.5.225	147	217 kB
10.10.100.43	151.101.193.140	125	154 kB
10.10.100.43	52.5.31.25	122	25 kB
10.10.100.43	151.101.129.140	118	114 kB
10.10.100.43	104.16.24.235	108	14 kB
10.10.100.43	23.192.15.138	107	91 kB
10.10.100.43	23.207.174.182	106	63 kB
10.10.100.43	151.101.1.140	106	30 kB
10.10.100.43	172.217.12.162	100	33 kB
10.10.100.43	173.241.242.143	96	21 kB
10.10.100.43	31.13.69.203	88	100 kB
10.10.100.43	172.217.10.225	84	26 kB
10.10.100.43	172.217.10.42	80	6 kB
10.10.100.43	52.94.232.32	76	18 kB
10.10.100.43	23.21.73.203	73	11 kB
10.10.100.43	23.207.173.144	69	41 kB

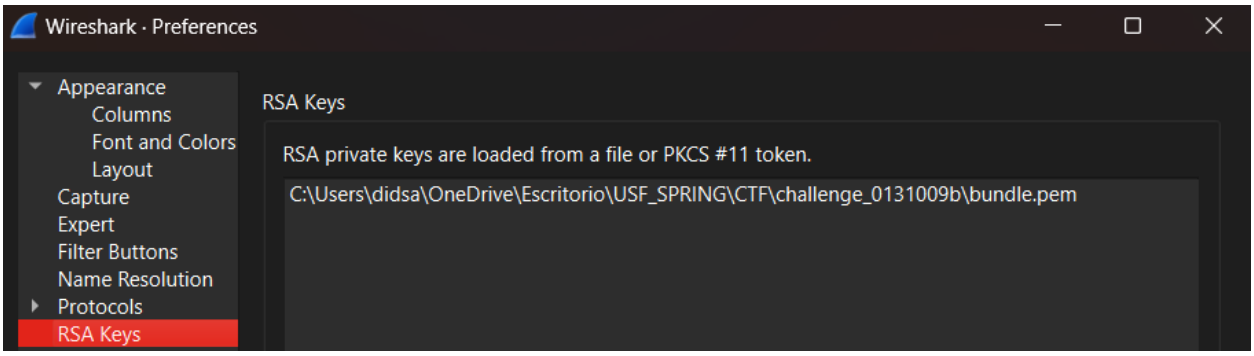
We can observe that the IP 10.10.100.43 is sending a lot of packets.

Now inside Wireshark I use a filter to see the packets that the IP is sending and receiving.

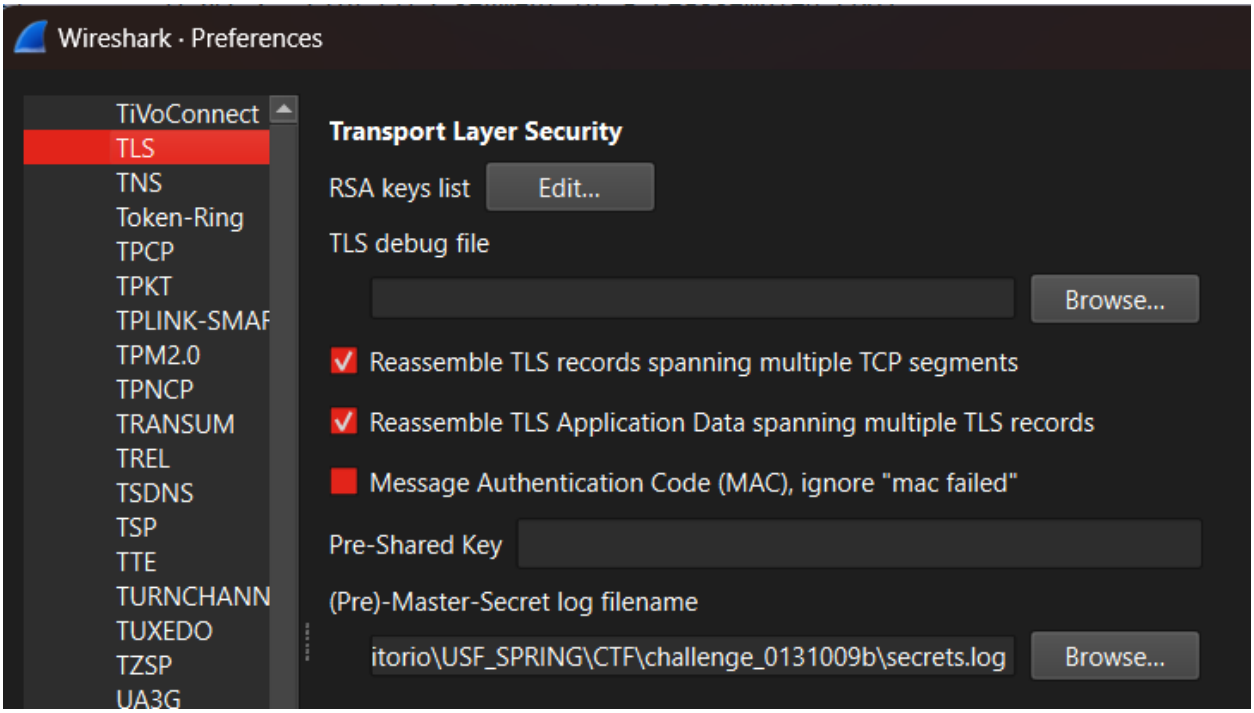
If I looked into an HTTP packet, I see that the port it is using is 443, which normally is used for HTTPS however it is using it for HTTP.

```
Transmission Control Protocol, Src Port: 49175, Dst Port: 443, Seq: 1, Ack: 1, Len: 292
    Source Port: 49175
    Destination Port: 443
```

Now. If we search TLS in the filter, everything shows as TLS. however, by changing the configuration of wireshark and using the secrets and bundle file we could configure the thing to divide the protocols and know the differences.

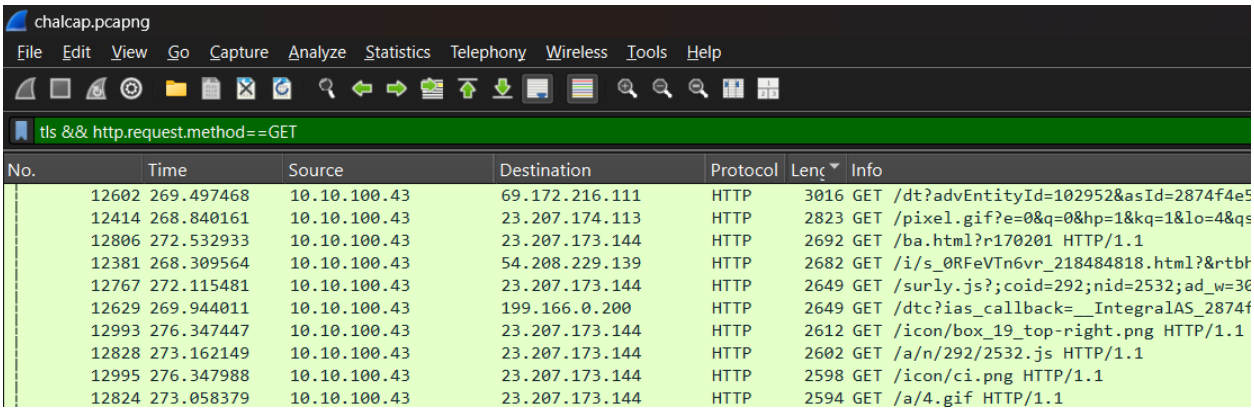


Here I put the keys that were inside the packet of the challenge. So now the specifics of the TLS configuration:



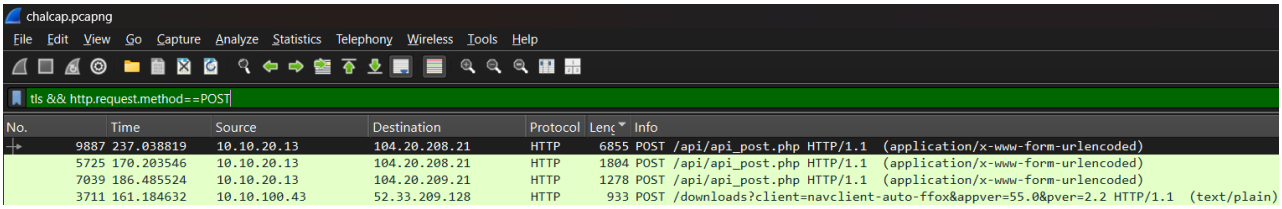
I input the secret file into the configuration of wireshark. With this set, now all the packets with the TLS filter are going to differentiate which is what we are looking for.

Now, we analyze the http method GET having them organized with length:

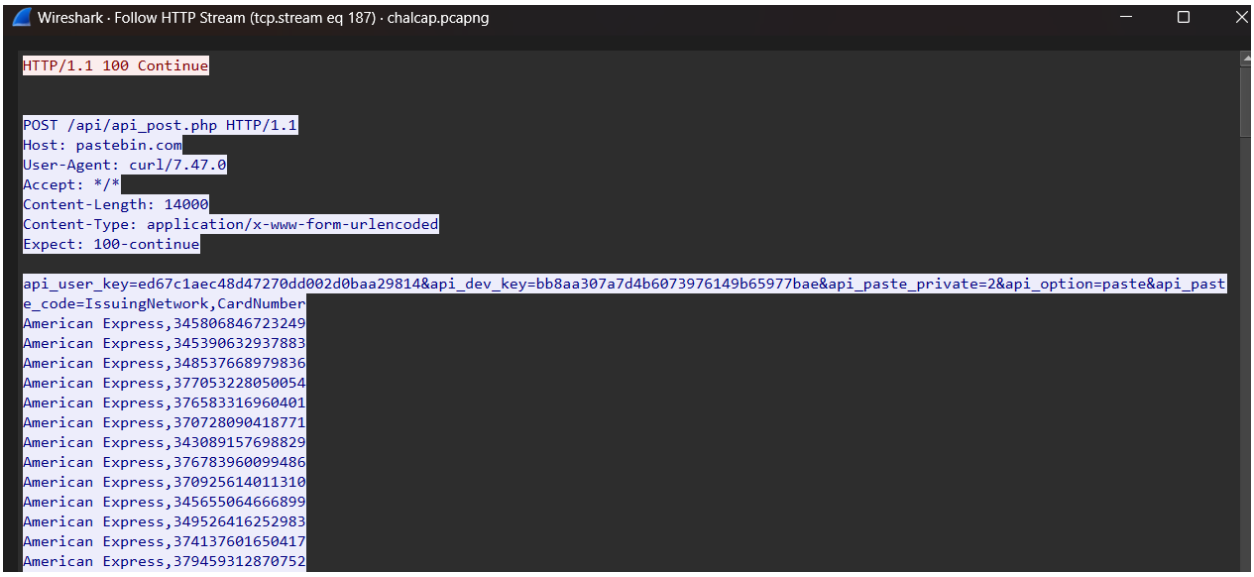


By analyzing different TCP streams of the packets, some of them didn't have anything suspicious, and others were just encrypted. Everything seemed normal.

Now I analyze the POST method



By following the TCP stream of the first packet we see this:



Inside of it we see credit cards information which is very suspicious and by going down we get the flag: HTB{Th15_15_4_F3nD3r_Rh0d35_M0m3NT!!