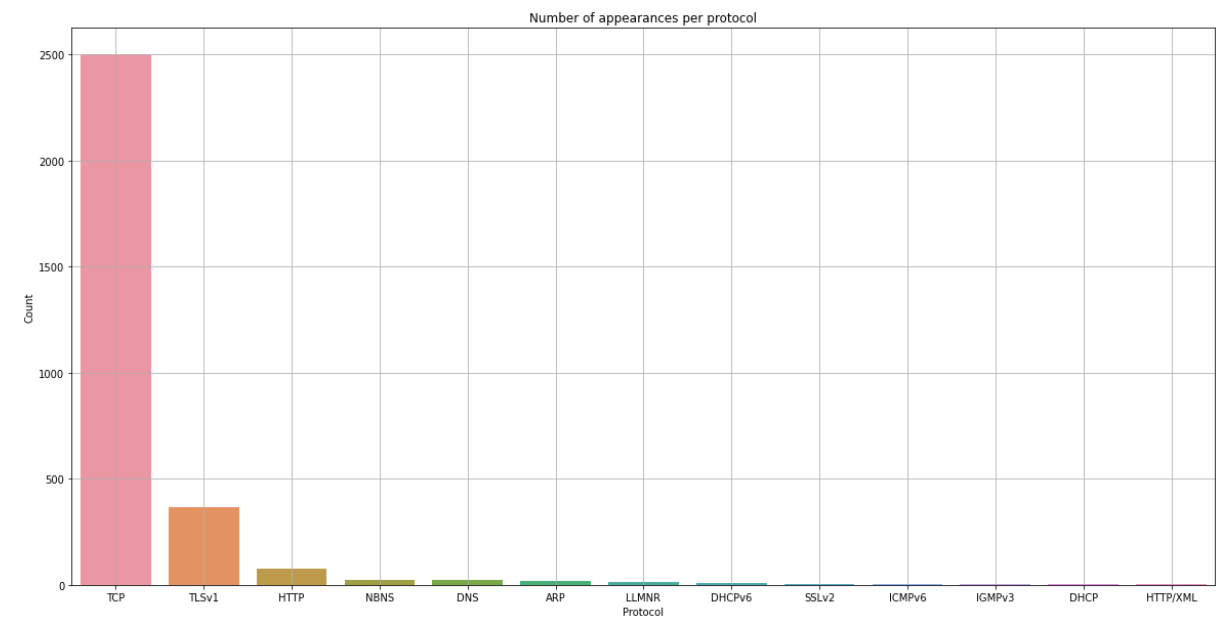
**Data Analysis in Security Assignment**

1. **Introduction**

The concept of cybersecurity is directly related to the network. According to ISO/OSI model, we should analyse the network regarding different layers containing various protocols. Network traffic itself is the perfect place to collect necessary data for such analysis. In order to gather raw data, we have used the network sniffer and network protocol analyser - Wireshark software. Subsequently, the data was extracted to the CSV file and analysed with Jupyter Notebook to provide a better understanding. The network traffic was simulated in a laboratory for educational purposes and published on the website malware-traffic-analysis.net in .pcap format which is readable with Wireshark.

1. **Protocol and Protocol Hierarchies**

Firstly, we needed to understand what type of protocols were used by the user in the captured network traffic. The graph generated by the Matplotlib library in Jupyter Notebook is shown in picture 2.1. Not surprisingly, the most used protocol is the TCP, which is a widely used reliable protocol in the transport layer.



*Picture 2.1 Appearances per protocol*

Obraz zawierający tekst

Opis wygenerowany automatycznieAccording to the graph the HTTP protocol was called during the activity. With the help of Wireshark, it is possible to analyse whether the API GET method was called and if so, get the file hashes of downloaded files. External software called VirusTotal analyses the potentially infected files. VirusTotal inspects items with over 70 antivirus scanners and URL/domain blocklisting services. Not only does it tell us whether a given antivirus solution detected a submitted file as malicious, but also displays each engine's detection label. In the pictures down below the files downloaded by the user, as well as the results of the analysis are shown.

*Picture 2.2 Sample files downloaded by user*

Obraz zawierający tekst

Opis wygenerowany automatycznieObraz zawierający tekst

Opis wygenerowany automatycznie

*Picture 2.3 Output from VirusTotal*

As a result, we detected that 2 out of 3 downloaded files by the user were infected with malicious software.