Hackathon 2021 autumn semester

Phishing attacks are everyday events nowadays. The attackers are trying to use more and more sophisticated methods to mislead the users. Besides using the conventional phishing channels such as emails, other ways of payload deliveries are getting more and more popular e.g. chat messages, SMSes, etc.

Not only the communication channel, but also the way how the user is misled has been developed a lot during the last years. Instead of sending a “Congratulations! You won an Iphone” type of message the attackers might send a “benign” like message from a spoofed sender first just to start the communication and send the malicious link in a later step.

The aim of the Hackathon is to develop a secure tool that is able to registers all type of phishing attempts and presents it to the analyzers. The analyzers want to identify phishing campaigns based on the registered message characteristics.

The functional requirements for the application:

- The application should be able to receive forwarded email, SMS and chat messages and parse these (sender email, phone, username, timestamp, malicious link, etc.).
- The application should be able to handle secure logins of analysts
- The application should be able to present the phishing data in a secure way (fetching data from the database and present it to the analyst) and provide options to add manual information to the data (add comments)
- The application should be scalable (able to receive large amount of data, handle several analyst with different roles)

General requirements:

- It should be a web based application
- Should be as secure as possible
- Source code and README file should be hosted on Github
- Prototype of the application should be deployed onSkyHiGh with a link to the floatingIP-address in the README file on Github
- Simple deployment guide with the application either in a single docker container or docker compose.