**Team Name:** Noble Team

**Current Leader:** Viren Kumar

**Members:** Melanie Brown, Marwan Elashry, Viren Kumar, Tanya Malik, Emily Nolan, and Lucas Scharf

**Melanie Brown:** I wasn’t able to get as much done. I worked on decrypting the TLS traffic in Wireshark using Burp Suite as a proxy. First I attempted to extract the shared secrets that are needed to decrypt. I haven’t been able to get it successfully yet. I tried to follow the steps from the shower thoughts, however that wasn’t successful. I plan to comb through the github page more to troubleshoot.

**Marwan Elashry:** Worked on decrypting the TLS traffic using the script provided by the previous team.

**Viren Kumar:** I was able to capture and save user inputted data into the webpage as a JSON object but can only view it locally within the console. Next steps would be to have the website hosted and store the data online for access anywhere. Also format the json inputted data better so we can have a massive list of usernames and passwords. Besides that, haven’t gotten much else done due to Thanksgiving break and 7 different 1500+ word papers.

**Tanya Malik:**

**Emily Nolan:** I didn't do much this week because I spent most of my time packing and moving but I did use the documents from last year on how to decrypt tls traffic by downloading and attaching the jar file from github and when I ran wireshark I was able to capture traffic but the documents from last year said I shouldve been able to see more details in the packets including WebSockerts and I did not see that so I think I did something wrong or missed a step before trying to capture data.

**Lucas Scharf:** I downloaded and attempted to decrypt the tls traffic on the fly using the Java script linked by the previous team. I was unable to get it working yet. I need to troubleshoot the wire shark tab where it says that a tls stream is empty. It’s hard to tell if the packets are decrypted when the stream is empty.