**Team Name:** Noble Team

**Current Leader:** Melanie Brown

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

**Melanie Brown:** I continued to research browser exploits and zero days from project zero. Researched more into what Lucas and Viren had done with the audio and TLS traffic to understand. Researched more on Burpsuite since I am not familiar with it to understand how to use it and its capabilities.

**Marwan Elashry:** Continued on working on Cortana’s functionality and project 0 by researching the CVEs. researched more about BurpSuite as well.

**Viren Kumar:** I continued attempted to decrypt TLS traffic by following a few YouTube videos. Worked on TLS decryption with Lucas. Links used: [Decrypting HTTPS Traffic With Wireshark](https://www.youtube.com/watch?v=a9eVf2uleaA&ab_channel=HackerSploit), [HTTPS Decryption with Wireshark // Website TLS Decryption](https://www.youtube.com/watch?v=GMNOT1aZmD8&ab_channel=DavidBombal).

**Tanya Malik:** I have been researching the four CVEs as part of Project 0, which are CVE-2017-5070, CVE-2020-6418, CVE-2019-5782, and CVE-2019-13764.

**Emily Nolan:**  I have been researching CVE 2020 15999 which is a Chrome Heap Buffer Overflow. It's not on the project 0 website but I found another blog about it and have been trying to follow their instructions on it. I also continued to read about and practice using Burpsuite.

**Lucas Scharf:** This week I continued the work on decrypting the captured audio packets from cortana. TLS decryption is still in progress. The CA certificate is still not working as intended. I am also struggling to understand the silk3 packet combination and conversion to mp3. I haven't found any resources online for this. Once TLS is decrypted we can move on to combination and conversion. I also researched Burpsuite.

**Future Direction Ideas:**

* Localized voice assistant or text assistant. Gets all the benefits of having a helpful cortana but not the risk of having info sent over the internet. Improved file search or something, no server calls. Processing done locally. Use for loops
* Complete Demo exploit from start to finish with TLS handshake capture and decryption. Using the previous groups streamlined Cortana packet editor that hopefully works more than 30% of the time.
* Researching what data the mistaken recording sends back.