**Team Name:** Noble Team

**Current Leader:** Marwan Elashry

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

**Melanie Brown:**

I worked on capturing the audio files using Wireshark this week. I ran into some trouble getting my Cortana working again. It was because I still had the manual proxy running from the exploit. After changing that I was able to log into Cortana again and have it respond to the voice activation. I ran the MITM attack again for the Kali and Windows VMs and started Wireshark to capture. Then I activated Cortana by wake word and asked a question and stopped the capture on Wireshark. The files were saved as .pcap. We can move forward using the .pcap file into decryption of the audio. We know the last team used a Java program to extract the shared secrets to decrypt the TLS. Lucas and I were looking into the encryption that’s used for the key exchange to possibly decrypt that way.

**Marwan Elashry:**

I kept working on recreating the CVE-2022-0337 and I was able to create a functional login page.

**Viren Kumar:**

I worked on developing the key logging algo in python. I also attempted to make it using JS and PHP. I ran into some trouble with getting the PHP and JS method working locally so I will probably have to host the site and run the script live. As for the python method, I have to compile the python script as an executable (.exe) in order for it to run in the background. A youtube video showed that all microsoft defender settings can be enabled as long as you transfer the .exe via flash drive rather than downloading it directly from an online source. If you want to download it directly, you do have to turn off Microsoft Active Defender in settings.

So far, I have the webpage remade, but I still need to find a cloud hosting provider. I can use the python key logging exe to post all keylogs made on the computer running the keylogger script to a remote server.

**Tanya Malik:**

I am looking at the Java code created by the previous group. I’m happy that it's almost Thanksgiving!

**Emily Nolan:**

I was working on extracting audio from Cortana through Wireshark. I was able to get the pcap files from Wireshark by asking Cortana a question and recording the interaction. I saved the pcap files from when the MITM was running as well as when it was not running by accident. I also recorded it by using the wake word and also by clicking the microphone button to see if the audio picked up more when I used the wake word. I have not been able to decrypt it yet but I have been looking into a similar method of last year using Java and also doing it by hand but I haven't found a clear way to do that yet. Also happy almost thanksgiving!!

**Lucas Scharf:**

Melanie and I are working on the decryption of TLS traffic and the combination of silk3 packets to create the mp3 file that is sent to Microsoft. Melanie was able to capture packets and we are currently analyzing them for what kind of TLS encryption they use for key exchange. I believe it will be Diffie-Hellman which means we will need to have the private keys ahead of time in order to decrypt this traffic. I have not identified a software we can use to combine the packets in order to create the audio file. The previous team says that they used java to remove some headers and create the file. I have looked in all the file exchanges and I don't see this code. Therefore we are exploring creating our own code to decrypt this traffic. This will take some time.