**Team Name:** Noble Team

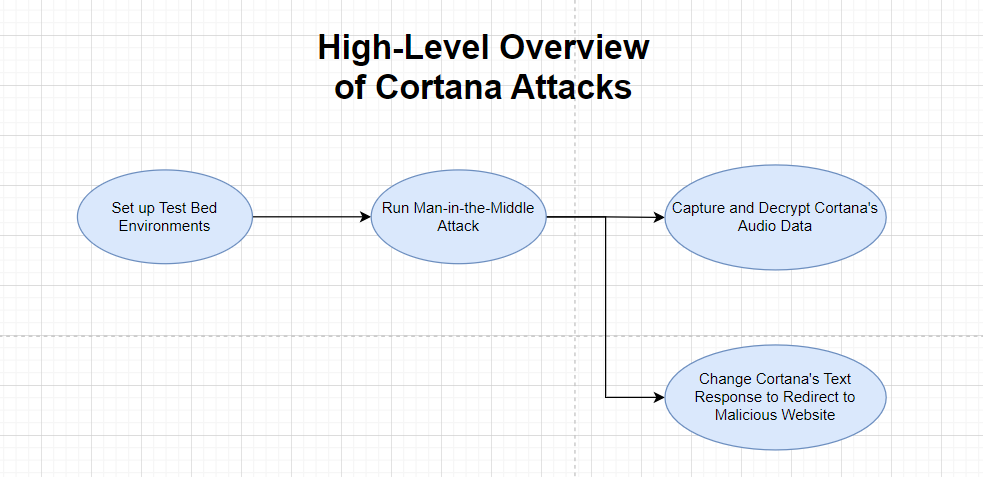
**Current Leader:** Viren Kumar

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

Zoom link for meeting: <https://gmu.zoom.us/j/99457453437?pwd=WTRIcjFIQXhJTklwRWNBaVl0L3NhUT09>

**Melanie Brown:**

I was able to update the high level overview to be small enough to put into the safe article later. I’ve mainly been working on the paper due tomorrow.



**Marwan Elashry:**

Trying to fix the code that Viren and Emily did not succeed in as of right now.

**Viren Kumar:**

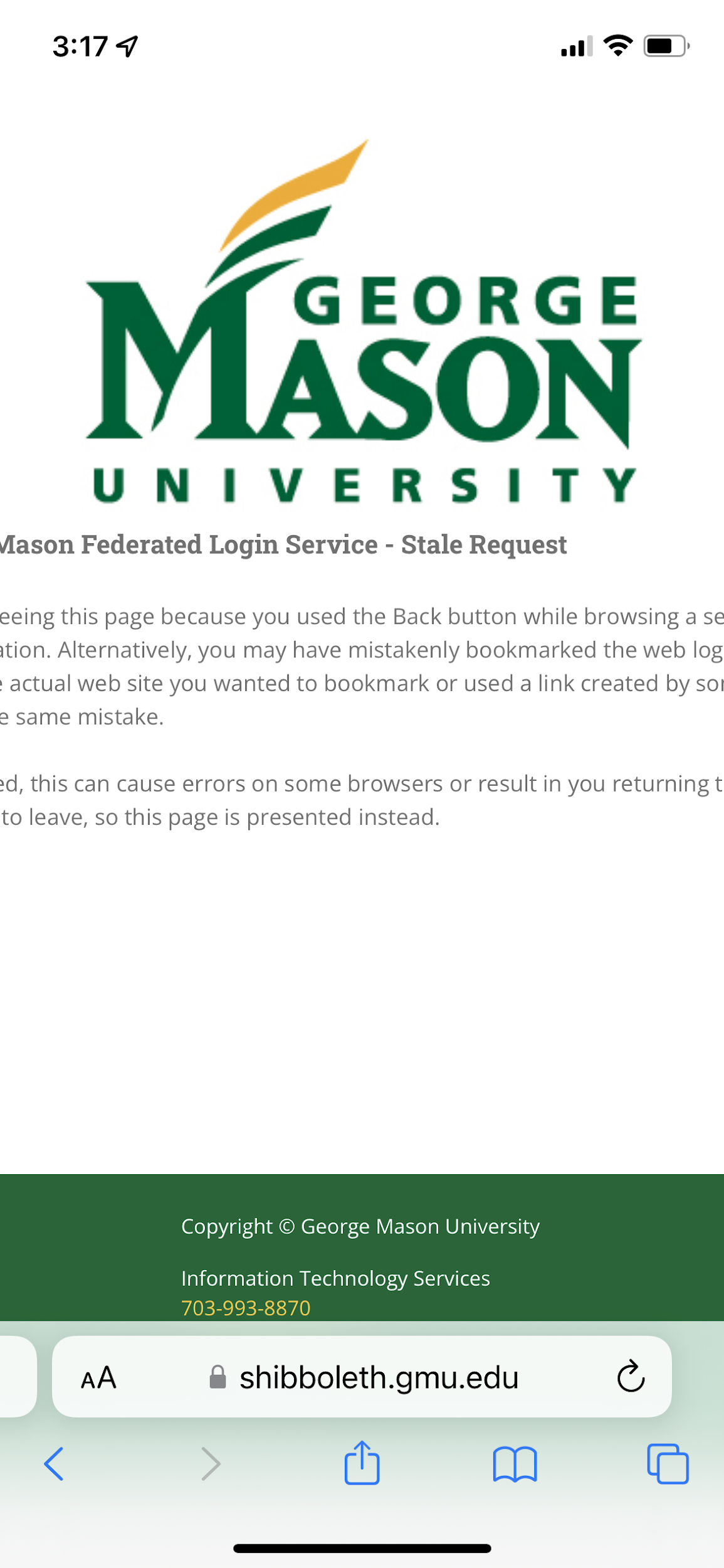
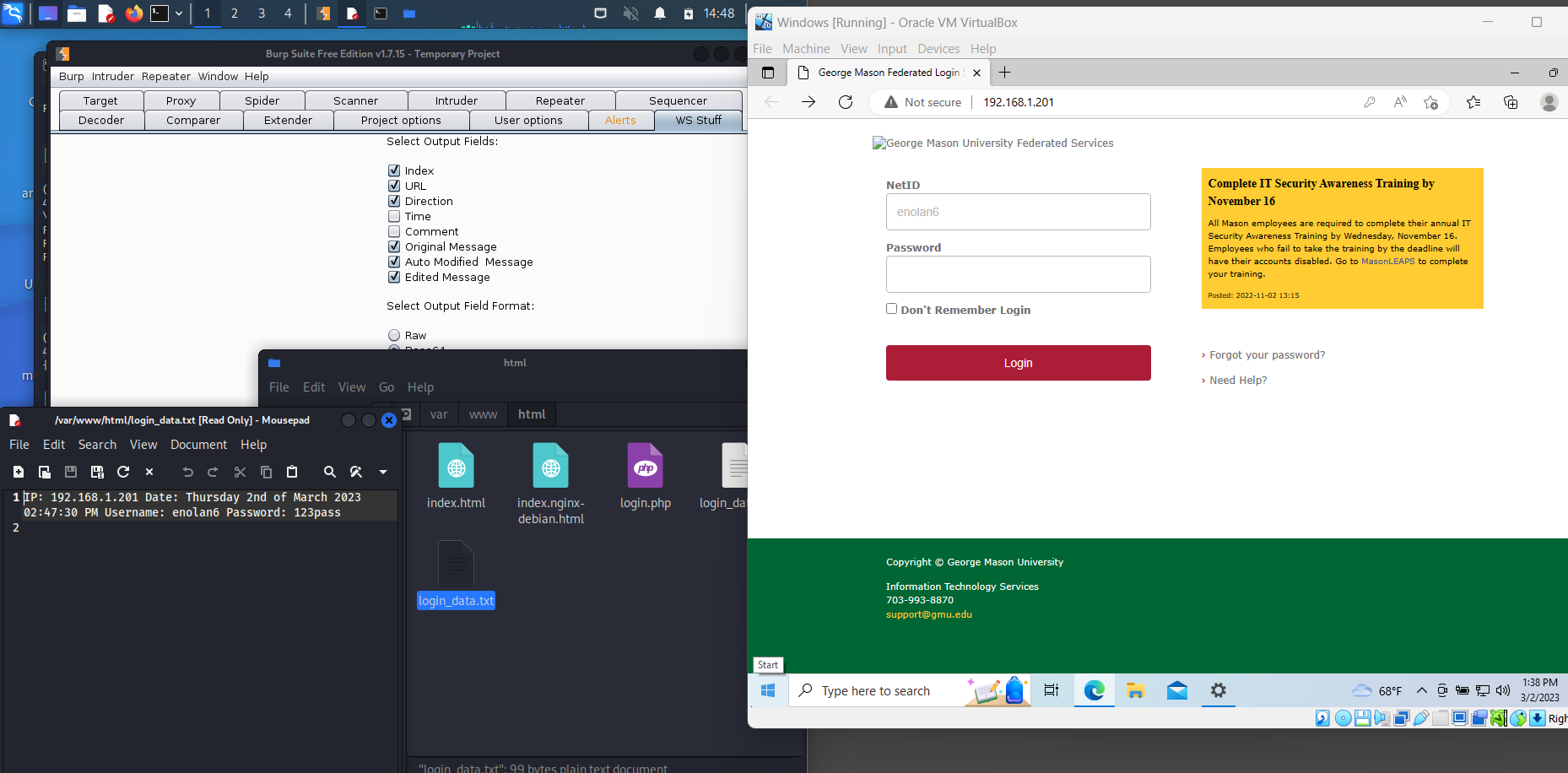
I reviewed the previous group's deliverables and code for any hints about getting the domain changed for the attack. Facing multiple errors that we are unsure how to fix. Worked with Emily to diagnose them, but still have no luck. Found the readme.txt file that we originally used to compile the code. Eventually, I was able to get the compiled code to work and it runs with no issues! All I had to do was look over the steps in the readme.txt a couple of times and found that I had the compressed feature on which was causing it not to work. After turning that off, it worked successfully! Lucas and I setup port forwarding rules and are now able to access the website from anywhere in the world as long as my apache2 server is running on my kali box, which adds a bit of security. The domain for the fake website is: gmu.hopto.org. I also added a useragent variable that pulls device information as well.

**Tanya Malik:**

Summary Here 2-3 sentences

**Emily Nolan:**

I was working on getting the Cortana attack to redirect to our website, not the blue halo one. We (Viren and I) tried compiling the code and saving it to a new file and using that one, we tried fixing some of the errors and warnings that popped up, and we tried to install a new certificate. We were using the readme file that came with the code folders and the shower thoughts doc section that talked about compiling to make sure we did it properly but none of these worked. It still takes us to the blue halo site. In the readme, they said that the only file that they edited was the evilfilter so I'm really not sure why it still takes us to the blue halo site even after we changed it and compiled it according to their instructions. BUT NOW IT WORKS. We got it to work today just now. EVERYTHING IS FINE



**Lucas Scharf:**

We got NoIP workingso that the website is no longer an ipaddress. It looks just like the actual website and forwards to a failed login page which could redirect to the official gmu login page. This could prevent suspicion and allow us to get away with credential stealing.

