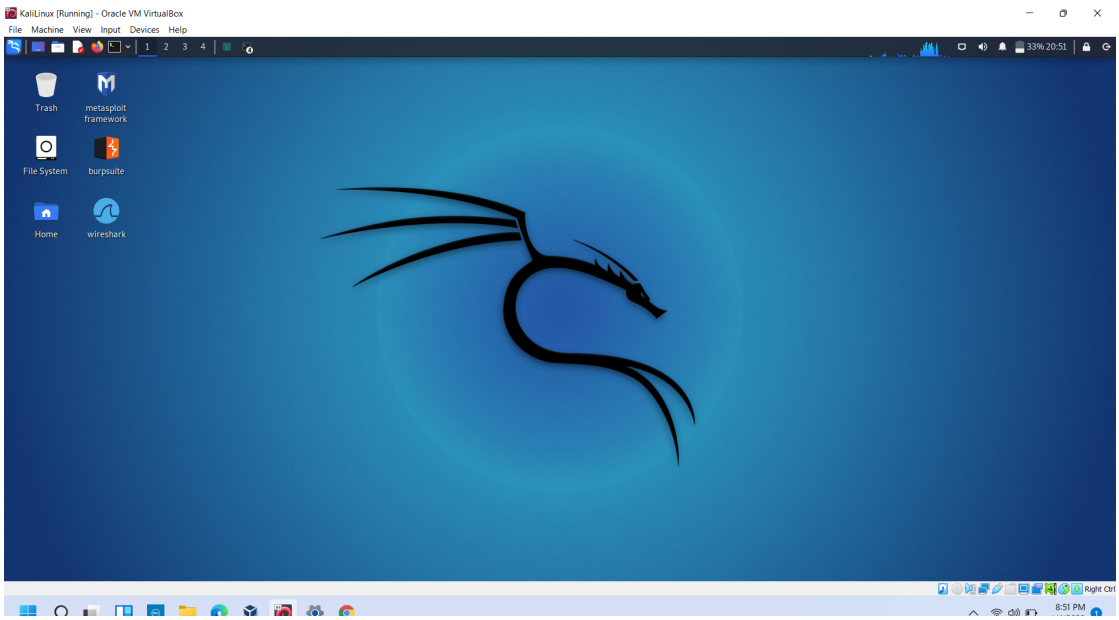
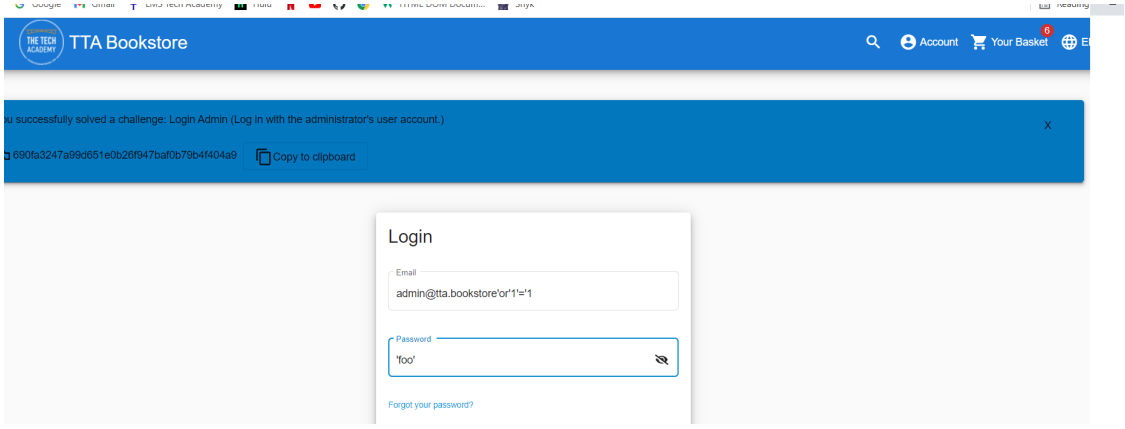
During my time with The Tech Academy I worked on a 2 week sprint live project following the Scrum ideology. Along with fellow colleagues, we helped solve real world problems and communicated our daily progress. We worked as a collective but were assigned individual tasks catering to our respective skills. I was assigned offensive and defensive security challenges such as analyzing malware traffic, penetration testing, inspecting pcap files and finding vulnerabilities in applications. Some of these challenges called for tools and techniques such as Wireshark, Burp Suite, SQL injections and privilege escalation attacks to name a few. Below are a few snippets of the challenges I completed along with incident reports describing my strategies.

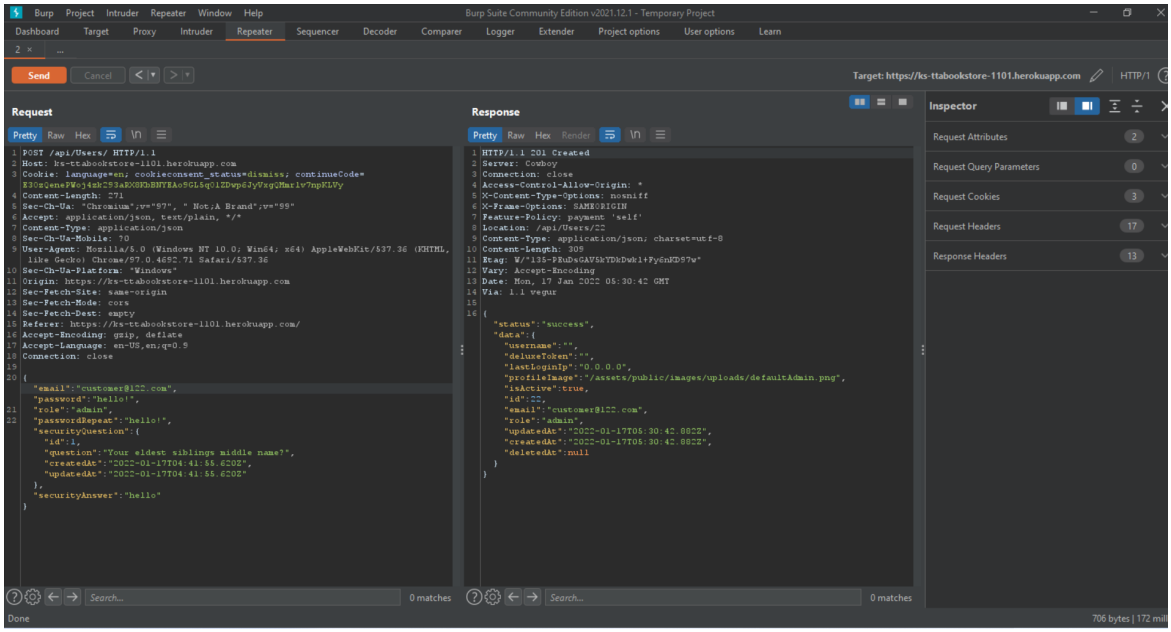
Most of these challenges I completed via VM VirtualBox using Kali Linux.



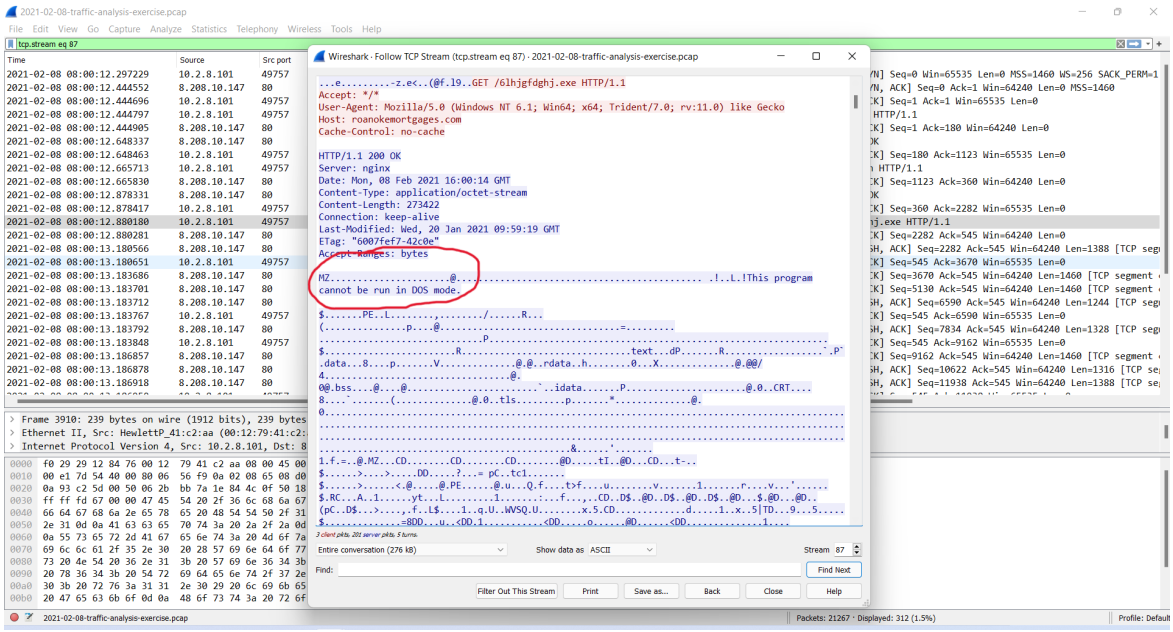
Here I'm using a SQL injection attack to gain administrative access.



I utilized the Burp Suite repeater tool to perform a privilege escalation attack.



Analyzed traffic using Wireshark to find malicious executables.



One of the incident reports I wrote after completing a challenge.

INCIDENT REPORT: KM-11087-Malware-Traffic
Date: 1-6-2022

Executive Summary:

A client's computer was infected with malware. I was given the task to find the source of the virus.

Results

Victim Details:

- **IP address:** 192.168.138.158
- **MAC address:** 00:00:5e.00.53.00 0x0806 (ARP)
- **Host name:** Windows NT 6.1
- **User account name:** unknown

Indicators of compromise(IOCs):

SHA256 hash: **396308a193041b87ce33be54f81429a79bf35ff7d7a38b998be7a8c435865350**

- File size: 560 bytes
- File type: PE32 executable (DLL)
- File descriptions: Win32:Crypt-SAR Trojan

Malicious HTTP traffic:

- 62.75.195.236 port 80 - GET /?b514ee6f0fe486009a6d83b035a4c0bd

Suspicious domains using HTTPS traffic:

- 188.165.164.184 port 49195 - ip-addr.es
- 72.34.49.86 port 49198 - comarksecuirty.com
- 204.152.254.221 port 49199 -runlove.us
- 95.163.121.204 port 49205 -gigapaysun.com

Completing these challenges has provided me with valuable experience that I will no doubt utilize on my path towards cyber security. With the skills I've gained during this course I'm confident I will be a valuable asset to any team.