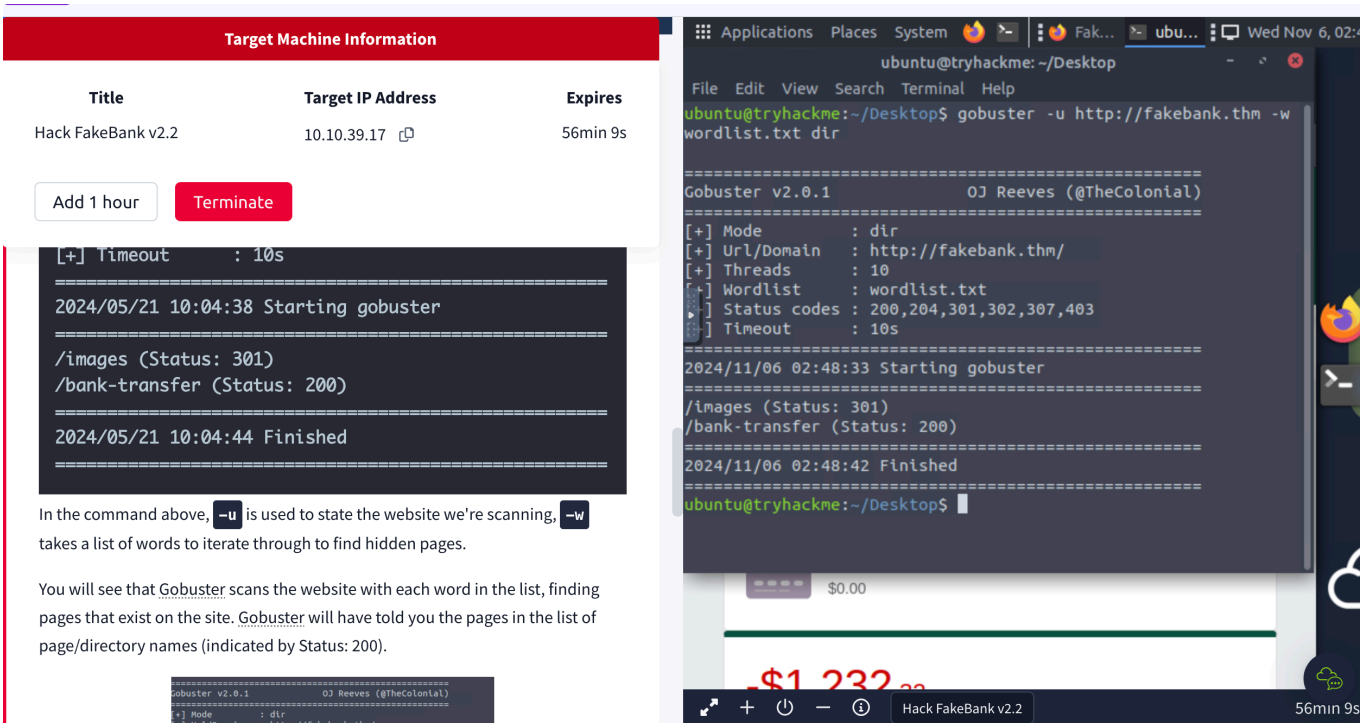
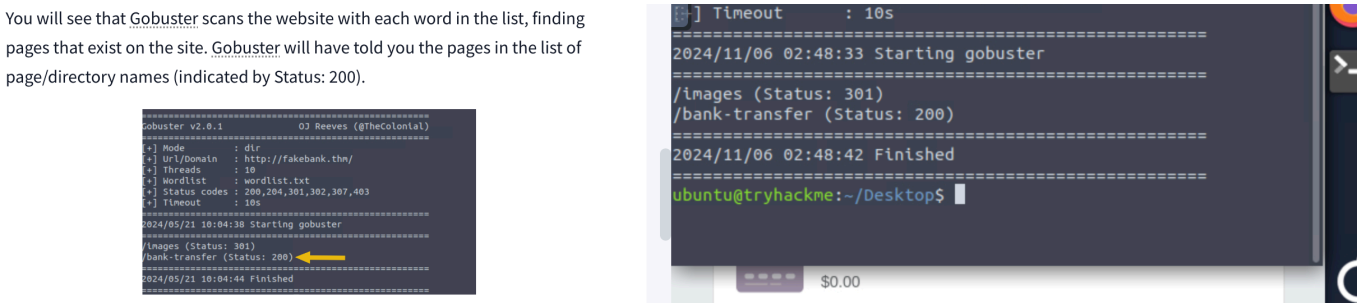
Intro to Offensive Security - Completed 11-05-24 & Documented 11-07-24

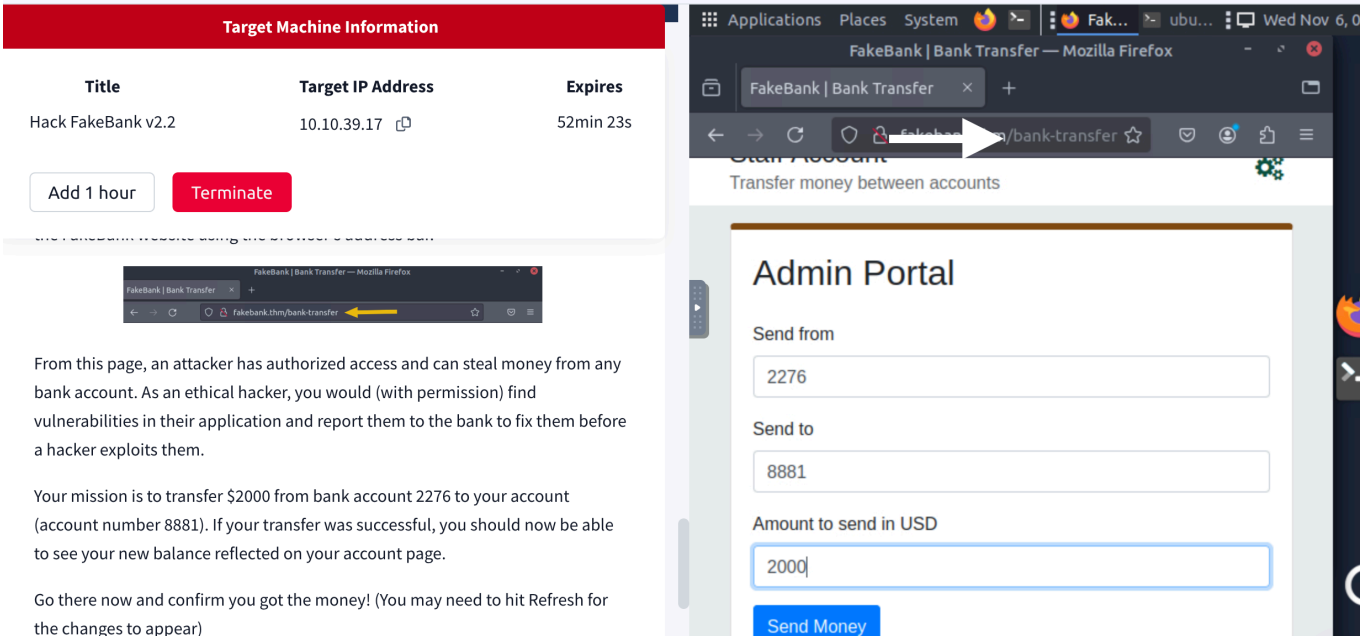
The first lab involves using a tool called 'gobuster' to scan a website for hidden directories, referencing specific words from a wordlist text file.



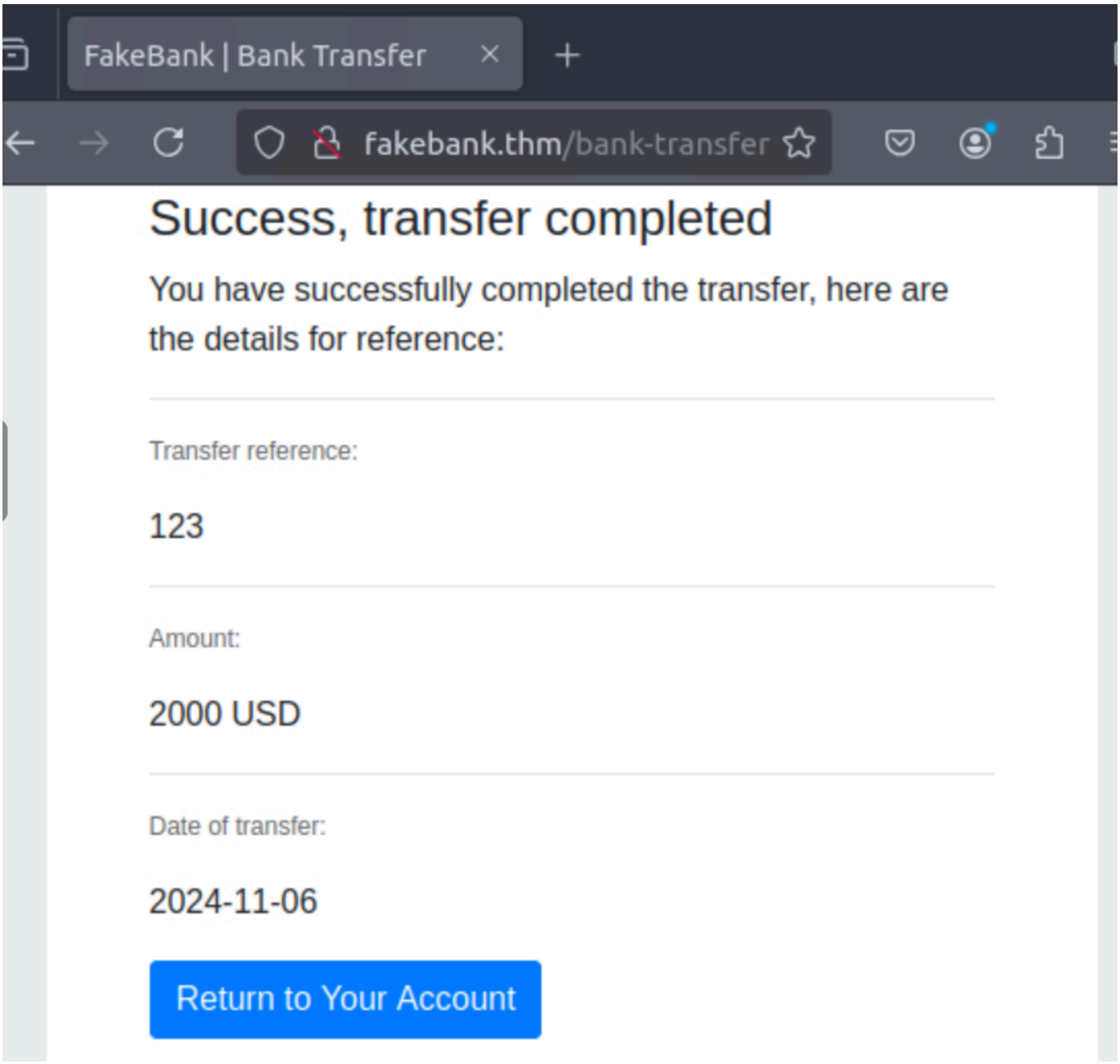
To the right, we ran the following command: gobuster -u http://www.websitename.xyz -w wordlist.txt dir
In this command:
-u specifies the URL we want gobuster to scan.
-w indicates the wordlist file (wordlist.txt) that gobuster will use to identify potential hidden directories.
'dir' is the mode, one of five offered by gobuster, that searches through each directory in the list for matches based on the conditions in our .txt file.



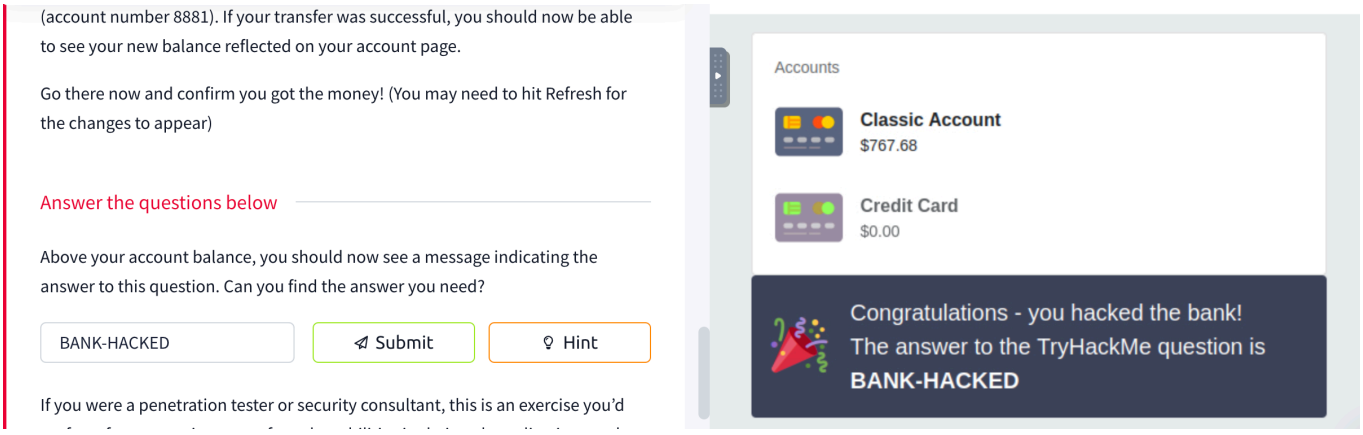
Between the start and finish messages on the right, we can see that gobuster has found two hidden directories from our wordlist: '/images' and '/bank-transfer.' The 'Status: 301' response indicates a redirection, showing us where the new /images page is located. The 'Status: 200' response indicates that our (GET) request to access the '/bank-transfer' path was successful.



After receiving the successful response, we navigated to the page by appending the path to the site's URL. Our next task was to transfer funds from the victim's account to our own.



Shortly after submitting the transfer request, we received a confirmation message.



Finally, we unlocked a message confirming the completion of our first TryHackMe learning path!

Additional resources:
https://www.freecodecamp.org/news/gobuster-tutorial-find-hidden-directories-sub-domains-and-s3-buckets/