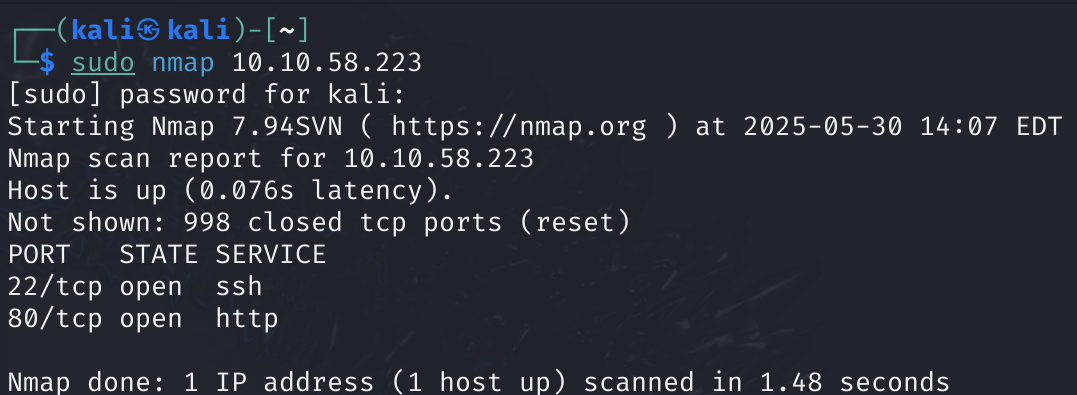
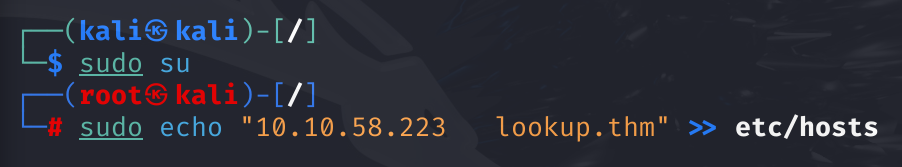
**Lookup\_Documentation**

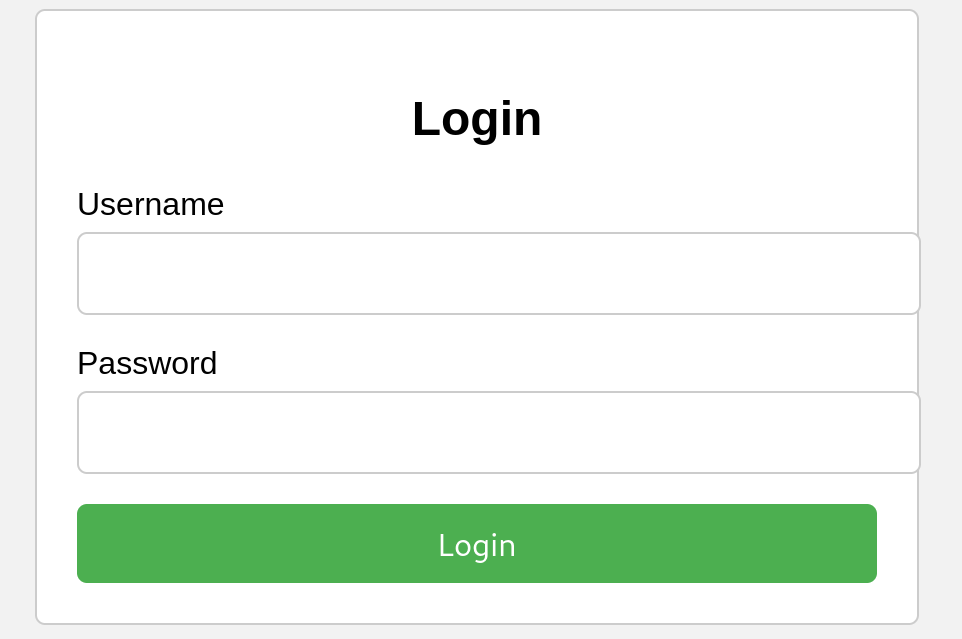
1. At the beginning, I scan the target’s open tcp top 1000 open ports using Nmap:



1. I realized that this target has an http open port, so I tried to enter the website. The problem was the domain lookup.thm wasn’t matched to the target’s IP. Therefore, I manually added to my machine’s hosts file the domain with the IP of the target by entering these commands:



1. After doing that, I opened that website again and this is the main page:



1. After some failed methods(like SQLi and XSS) to find the right credentials, I moved to write this Python script to enumerate usernames over the system:

תמונה שמכילה טקסט, חשמל, צילום מסך, תצוגה

תוכן שנוצר על-ידי בינה מלאכותית עשוי להיות שגוי.

After running this script, I found an existing username named “admin”.

1. Now, I changed a little the script to find the password of the username “admin”: