Going on port 80, there is the default apache2 installation page so I need a hostname to progress. I add bank.htb to the /etc/hosts file. I then run gobuster with wordlist 2.3-medium and see that there is an extension called balance-transfer. I sort the data by size of file and see that one of the is unencrypted. Using chris' credentials, I log into his bank account. I try different methods of uploading a jpg php exploit including renaming the file with extensions like .php.jpg and tools like exiftool
(https://www.ired.team/offensive-security-experiments/offensive-security-cheetsheets) but after intercepting the error request using Burpsuite, I saw that a .htb extension runs php code. So I uploaded shellcode with the extension .htb and got a reverse connection. Using the command find / -user -4000 2>/dev/null I find an executable called emergency which gives me root. An alternative was to create a new password using the command:
openssl passwd password
which gives us a crypt password and editing the /etc/passwd file with the hash value gives us ssh access to root using password "password".