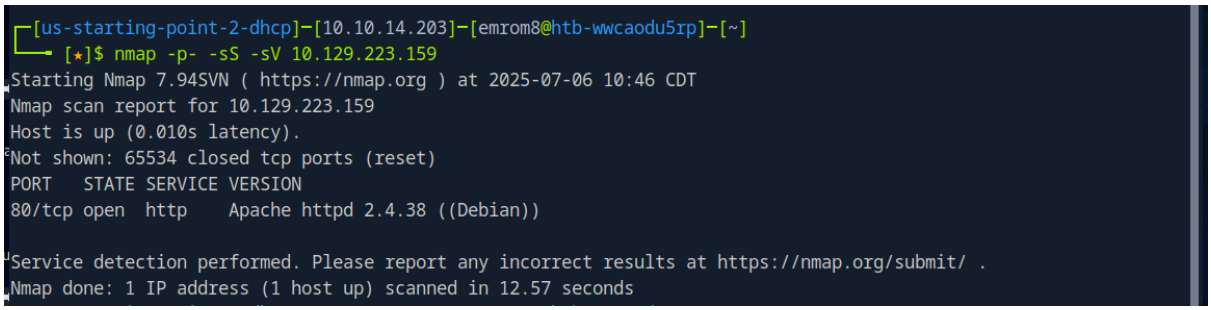
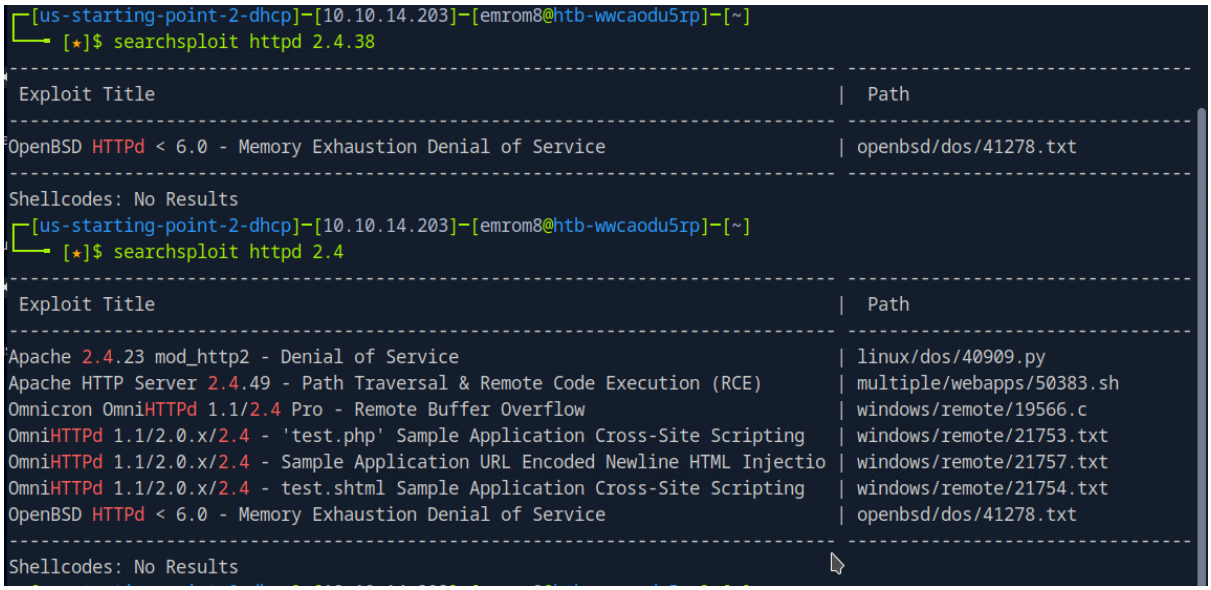
Our target machine here is 10.129.223.159 – as always, let's start with our basic nmap scan:



Let's see what exploits are potentially available for the service on port 80:



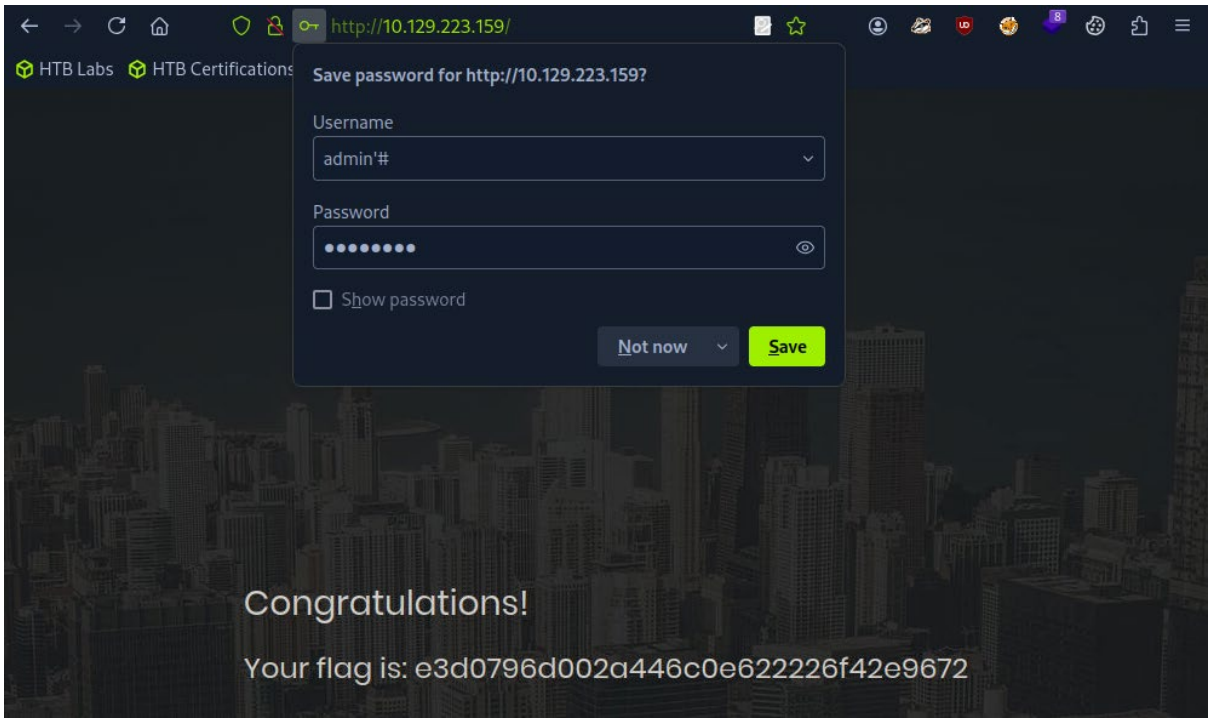
We know this service is running on port 80, so let's access it from our browser and try to login:

Attempt 1 Brute Force: username = admin, password= admin → Unsuccessful

Attempt 2 SQL Injection: username= ' OR 1'=1', password= irrelevant → Unsuccessful

Attempt 3 SQL Injection: username= admin, password = ' OR 1'=1' → Unsuccessful

Attempt 4 SQL Injection: username= admin'#, password= irrelevant → Successful



The reason this worked as an SQL injection is because the script input in the username field terminates the SQL injection query early and comments the rest of the query bypassing the password check. The dependency that is script relies on is the assumptions that a user named 'admin' exists.

Another machine down!