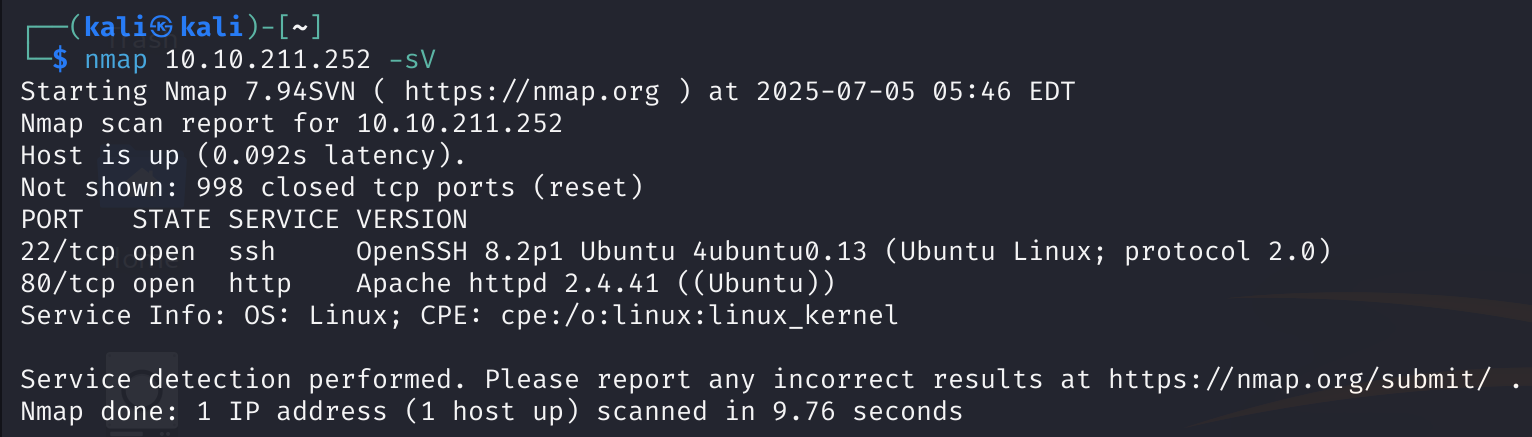
**Publisher\_Solution\_Documentation**

**Written by: Yuval Quina**

1. To begin with, I started the challenge with performing a basic port and services enumeration using Nmap:

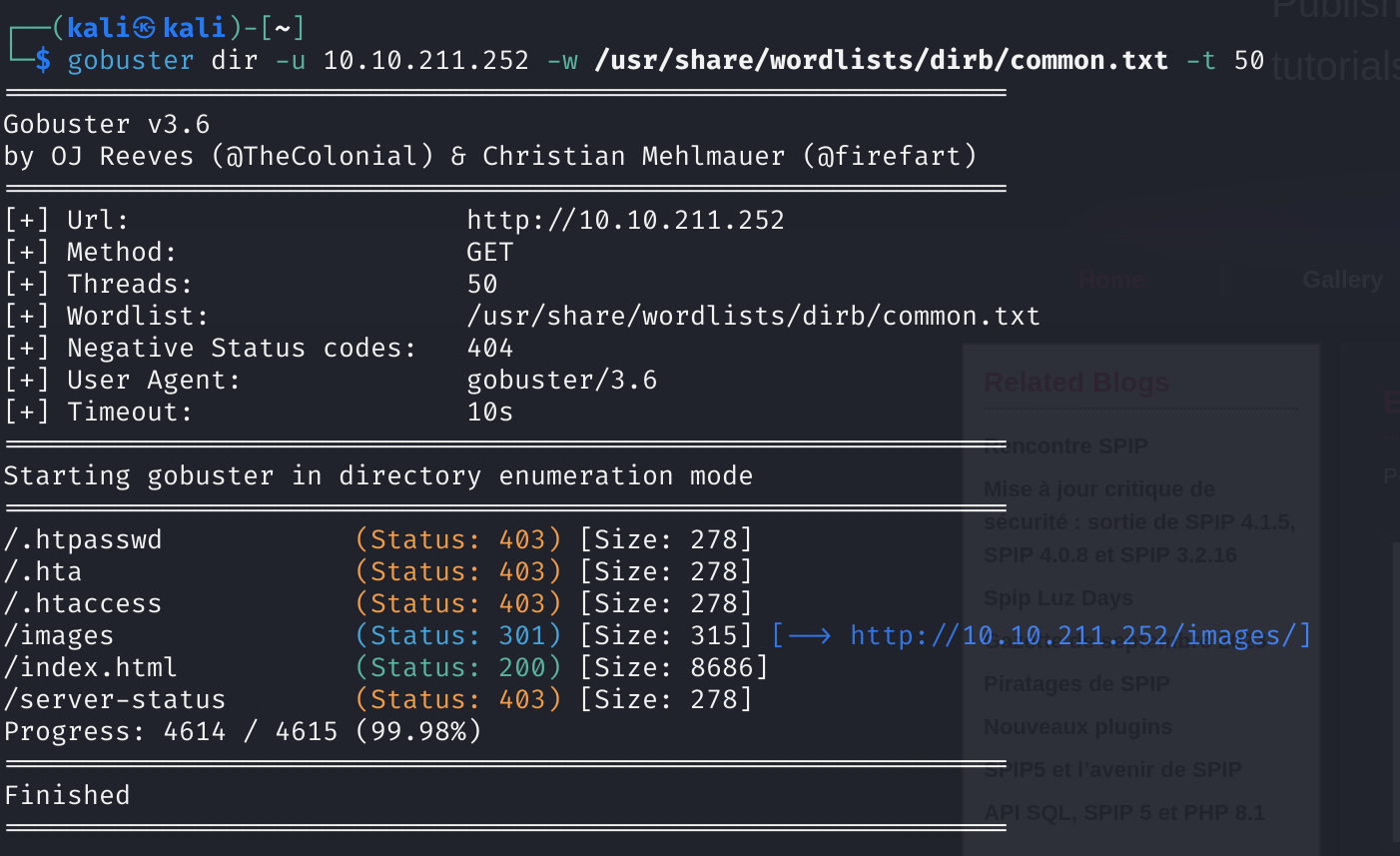
\

And immediately after doing it I opened the target’s website(because of the open 80 port):



Now, I investigated a little the website and found that most of the button doesn’t do anything and that it’s useless.

After doing it, I enumerated directories using “gobuster” utility and I found several pages and directories:



I understood that the 403 error status pages are shown as forbidden because of me being unauthorize to access them so I entered the “/index.html” and the directory “/images/”:



The “/index.html” move me back to the home page.

תמונה שמכילה טקסט, חשמל, צילום מסך, תוכנה

תוכן בינה מלאכותית גנרטיבית עשוי להיות שגוי.

And the “/images/” directory led me to the file system of the target machine, but it didn’t help me too much.

1. Now, I looked again on the website and realized that many times that name “SPIP” appears, so I check it on google and found the this is a “system for publishing content on the internet“ which is a platform to develop websites in this case. I did one plus one and realized that the target’s website probably built over this service, so I just need to find its exact version in order to find an exploit for that.

I started with