**“UnderPass” HTB CTF – Solution**

1. First of all, I performed a basic port scanning using **Nmap** by this command:

$ sudo nmap -sV 10.10.11.48 -Pn -oN "basic\_port\_scan.txt"

The results are:

# Nmap 7.94SVN scan initiated Tue Feb 11 14:51:36 2025 as: /usr/lib/nmap/nmap -sV -Pn -oN basic\_port\_scan.txt 10.10.11.48

Nmap scan report for 10.10.11.48

Host is up (0.13s latency).

Not shown: 998 closed tcp ports (reset)

PORT STATE SERVICE VERSION

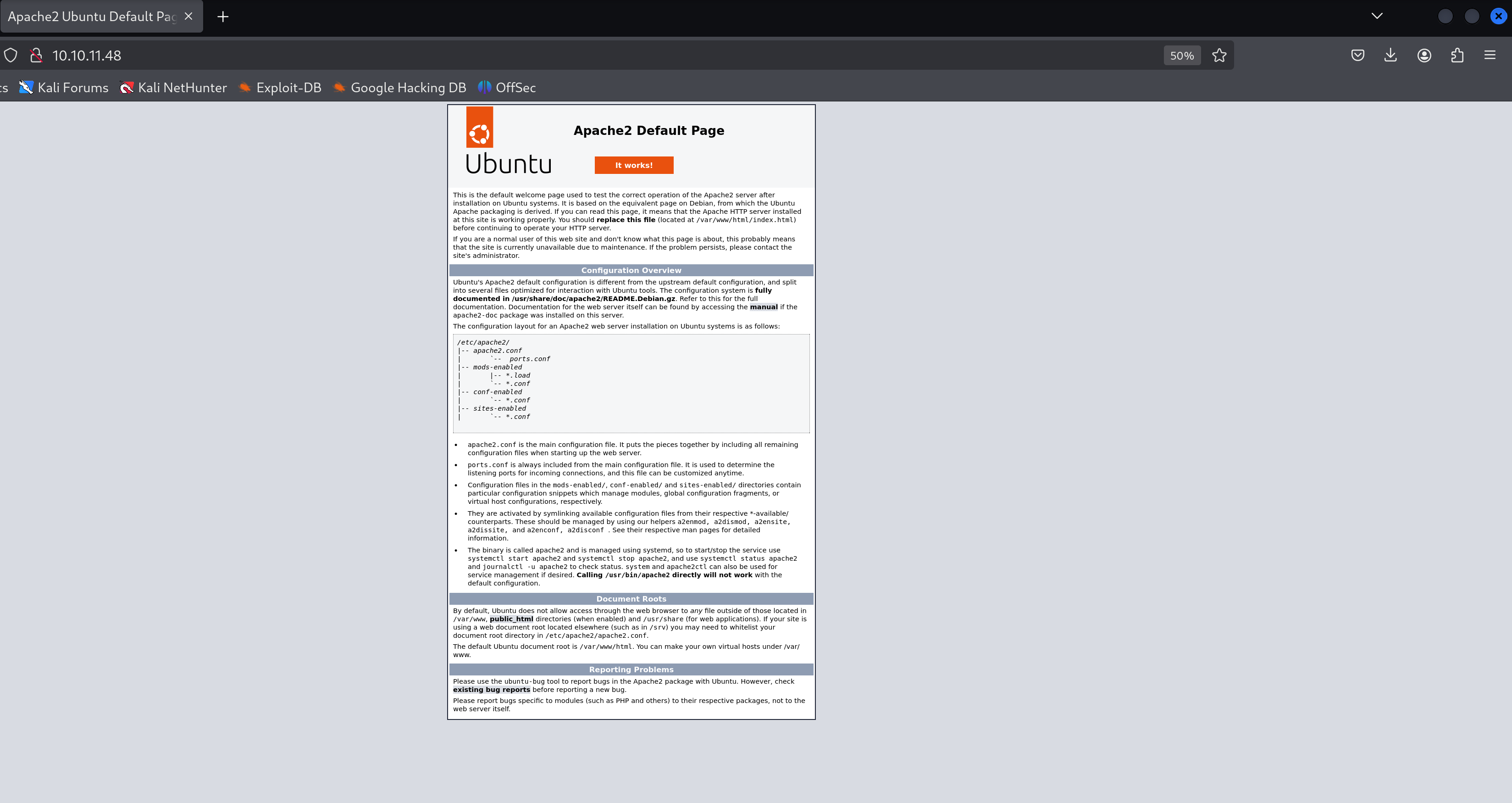
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)

80/tcp open http Apache httpd 2.4.52 ((Ubuntu))

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

# Nmap done at Tue Feb 11 14:51:45 2025 -- 1 IP address (1 host up) scanned in 9.23 seconds

1. Then I entered the website of the target using **port 80** which looks like this: 
2. I tried to enter the **inspector mode**, but I found nothing special.
3. Then, I tried to use the open **ssh port** in order to get a reverse shell over the machine and get access to it.
4. Therefore, I try to use the **ssh** tool over the machine, but I realize that I need the **username and the password**.
5. This made me think of trying different approach and try and scanning **UDP** ports using this Nmap command:

sudo nmap -sU 10.10.11.48 -Pn -n --disable-arp-ping -T5

The results are:

Nmap scan report for 10.10.11.48

Host is up (0.075s latency).

Not shown: 518 closed udp ports (port-unreach), 481 open|filtered udp ports (no-response)

PORT STATE SERVICE

161/udp open snmp

Nmap done: 1 IP address (1 host up) scanned in 556.25 seconds

1. The open snmp led me to use the