**“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

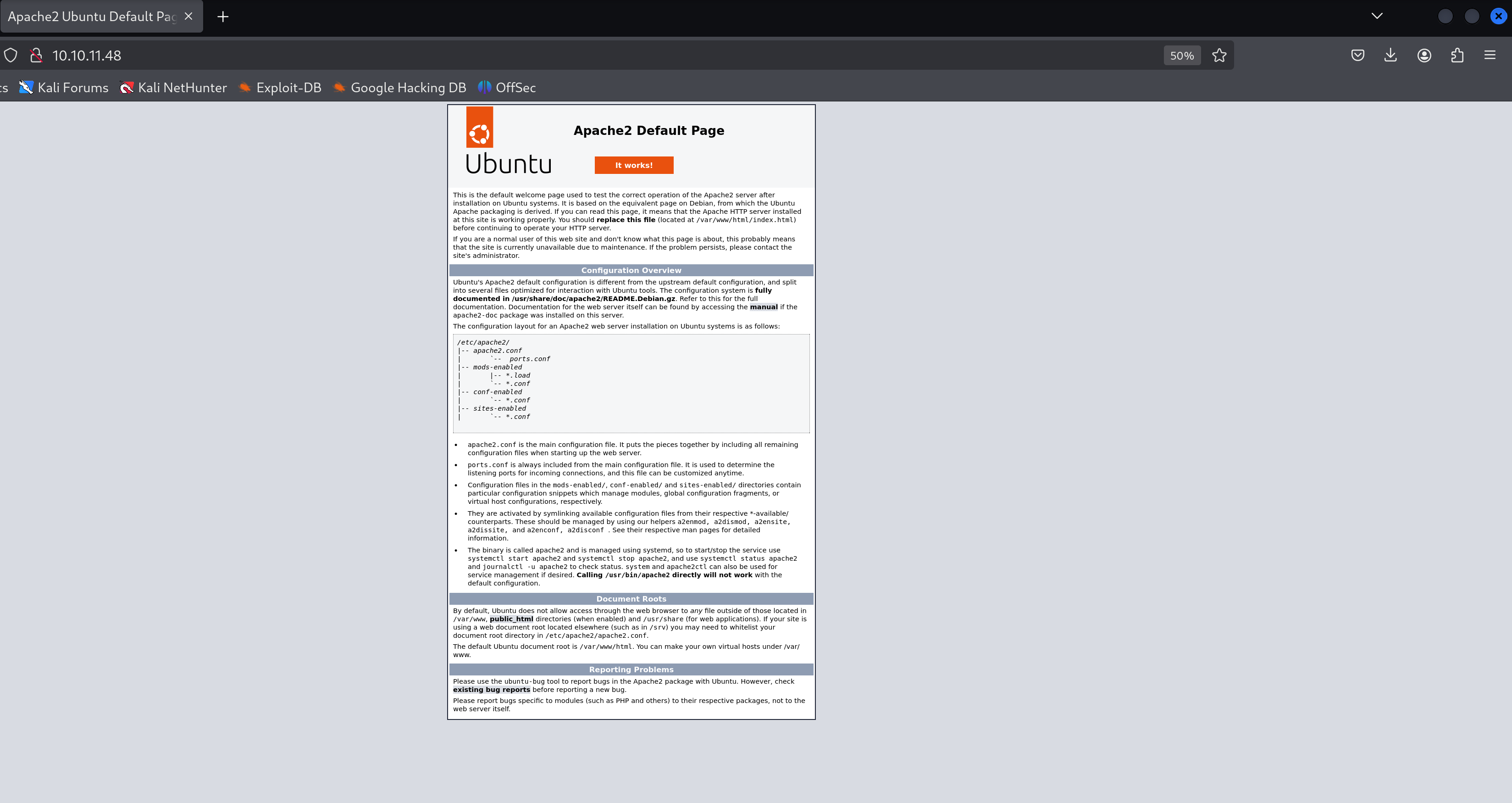
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)

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.
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 (a protocol which is used to network monitoring and management)** port led me to use the **SnmpWalk** Linux tool in order to get more data about the machine host by entering the following command:

$ snmpwalk -v1 -c public 10.10.11.48

The results are:

iso.3.6.1.2.1.1.1.0 = STRING: "Linux underpass 5.15.0-126-generic #136-Ubuntu SMP Wed Nov 6 10:38:22 UTC 2024 x86\_64"

iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10

iso.3.6.1.2.1.1.3.0 = Timeticks: (1149184) 3:11:31.84

iso.3.6.1.2.1.1.4.0 = STRING: "steve@underpass.htb"

iso.3.6.1.2.1.1.5.0 = STRING: "UnDerPass.htb is the only daloradius server in the basin!"

iso.3.6.1.2.1.1.6.0 = STRING: "Nevada, U.S.A. but not Vegas"

iso.3.6.1.2.1.1.7.0 = INTEGER: 72

iso.3.6.1.2.1.1.8.0 = Timeticks: (7) 0:00:00.07

iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1

iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1

iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1

iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1

iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.16.2.2.1

iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.49

iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.50

iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.2.1.4

iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.6.3.13.3.1.3

iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.2.1.92

iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The SNMP Management Architecture MIB."

iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The MIB for Message Processing and Dispatching."

iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The management information definitions for the SNMP User-based Security Model."

iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for SNMPv2 entities"

iso.3.6.1.2.1.1.9.1.3.5 = STRING: "View-based Access Control Model for SNMP."

iso.3.6.1.2.1.1.9.1.3.6 = STRING: "The MIB module for managing TCP implementations"

iso.3.6.1.2.1.1.9.1.3.7 = STRING: "The MIB module for managing UDP implementations"

iso.3.6.1.2.1.1.9.1.3.8 = STRING: "The MIB module for managing IP and ICMP implementations"

iso.3.6.1.2.1.1.9.1.3.9 = STRING: "The MIB modules for managing SNMP Notification, plus filtering."

iso.3.6.1.2.1.1.9.1.3.10 = STRING: "The MIB module for logging SNMP Notifications."

iso.3.6.1.2.1.1.9.1.4.1 = Timeticks: (5) 0:00:00.05

iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (5) 0:00:00.05

iso.3.6.1.2.1.1.9.1.4.3 = Timeticks: (5) 0:00:00.05

iso.3.6.1.2.1.1.9.1.4.4 = Timeticks: (5) 0:00:00.05

iso.3.6.1.2.1.1.9.1.4.5 = Timeticks: (5) 0:00:00.05

iso.3.6.1.2.1.1.9.1.4.6 = Timeticks: (5) 0:00:00.05

iso.3.6.1.2.1.1.9.1.4.7 = Timeticks: (5) 0:00:00.05

iso.3.6.1.2.1.1.9.1.4.8 = Timeticks: (5) 0:00:00.05

iso.3.6.1.2.1.1.9.1.4.9 = Timeticks: (7) 0:00:00.07

iso.3.6.1.2.1.1.9.1.4.10 = Timeticks: (7) 0:00:00.07

iso.3.6.1.2.1.25.1.1.0 = Timeticks: (1151148) 3:11:51.48

iso.3.6.1.2.1.25.1.2.0 = Hex-STRING: 07 E9 02 0F 12 2E 31 00 2B 00 00

iso.3.6.1.2.1.25.1.3.0 = INTEGER: 393216

iso.3.6.1.2.1.25.1.4.0 = STRING: "BOOT\_IMAGE=/vmlinuz-5.15.0-126-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro net.ifnames=0 biosdevname=0

"

iso.3.6.1.2.1.25.1.5.0 = Gauge32: 1

iso.3.6.1.2.1.25.1.6.0 = Gauge32: 222

iso.3.6.1.2.1.25.1.7.0 = INTEGER: 0

End of MIB

1. From the output I found this string: “**steve@underpass.htb**” which seems like an email address and from the username part of the address I found the username of the machine named “**steve**”.
2. Now, I can start bruteforce the machine **ssh** service using **hydra** tool: