Primer Taller Seguridad

Brahyam Hurtado Quiceno

240220191016

Institución Universitaria EAM

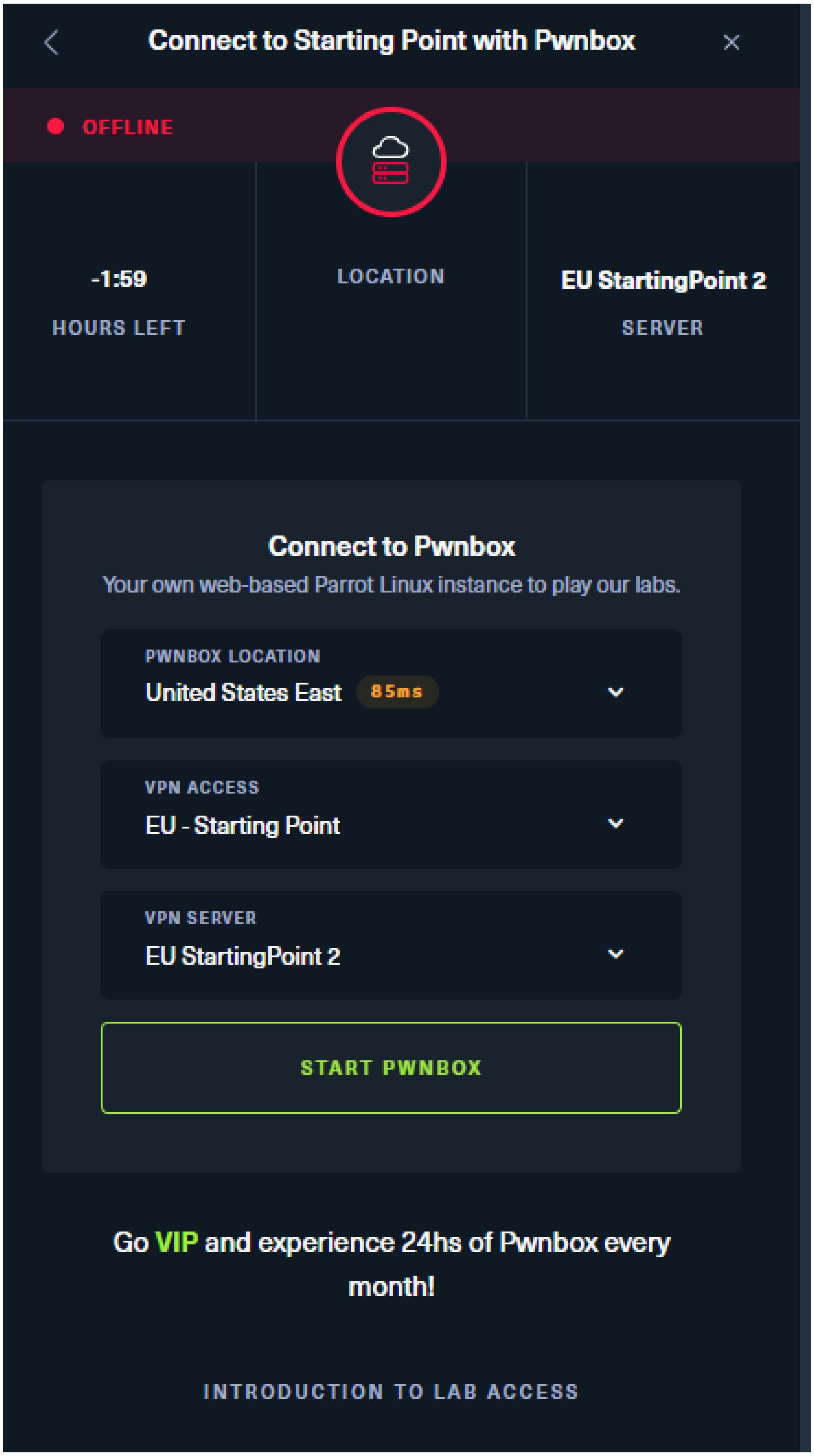
SNIES: 52410 Ingeniería de software

Seguridad

Johan Sebastian Giraldo Hurtado

25/02/2024

1. Empezamos por entender cómo usar la VPN de HackTheBox



Connect to Starting Point with Pwnbox

OFFLINE

-1:59 HOURS LEFT

LOCATION

EU StartingPoint 2 SERVER

Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

PWNBOX LOCATION: United States East 85ms

VPN ACCESS: EU - Starting Point

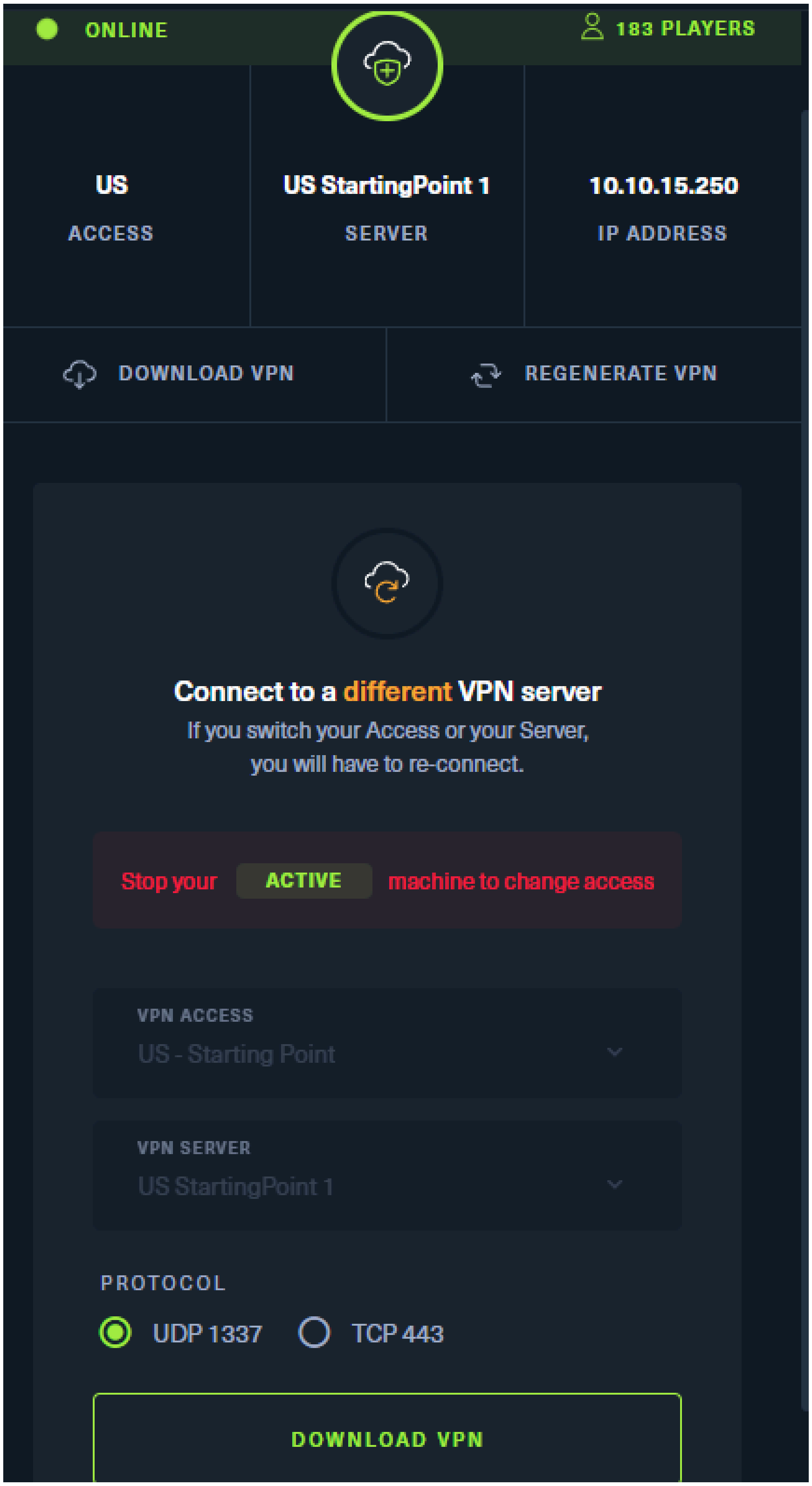
VPN SERVER: EU StartingPoint 2

START PWNBOX

Go VIP and experience 24hs of Pwnbox every month!

INTRODUCTION TO LAB ACCESS

2.



US
ACCESS

US StartingPoint 1
SERVER

10.10.15.250
IP ADDRESS

Connect to a different VPN server

If you switch your Access or your Server,
you will have to re-connect.

Stop your ACTIVE machine to change access

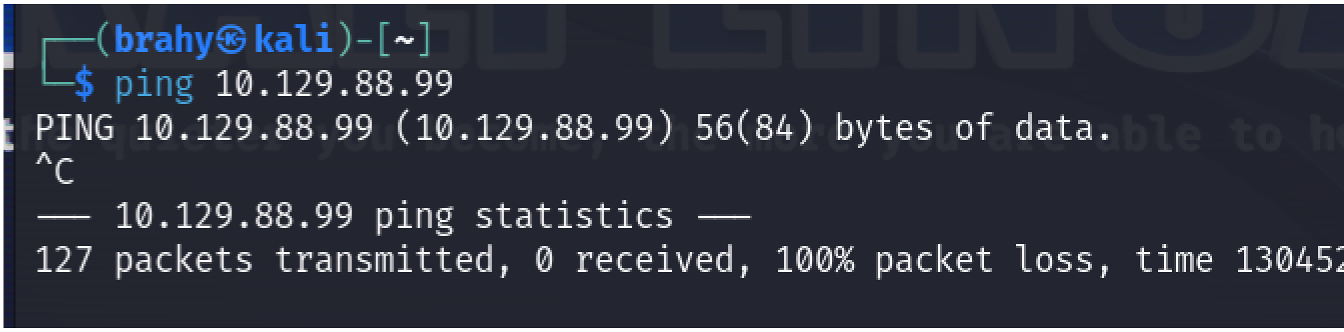
VPN ACCESS
US - Starting Point

VPN SERVER
US StartingPoint 1

PROTOCOL

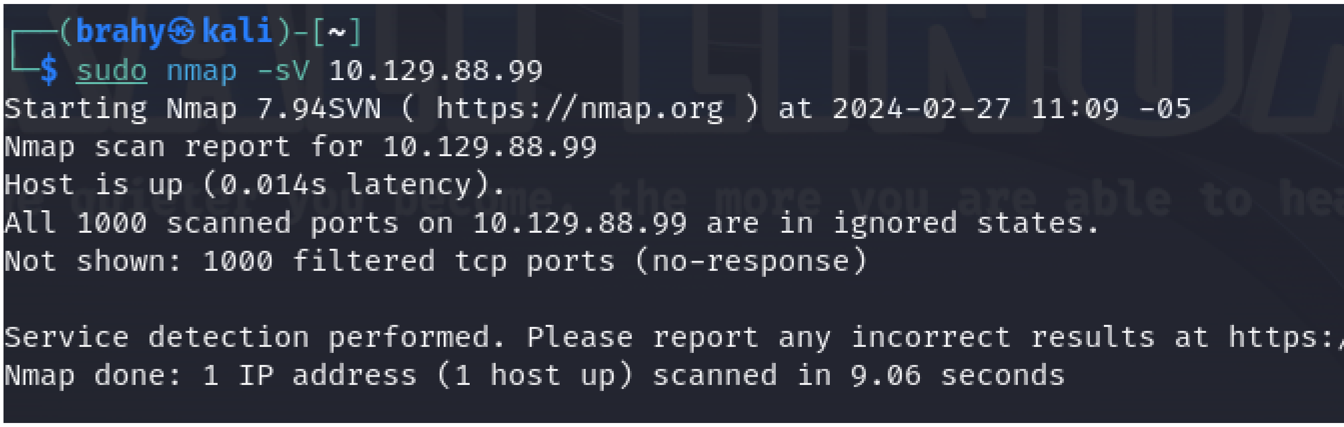
● UDP 1337 ○ TCP 443

3. Hacemos un ping a la IP a reconocer la cual es 10.129.88.99



```
┌──(brahy㉿kali)-[~]
└─$ ping 10.129.88.99
PING 10.129.88.99 (10.129.88.99) 56(84) bytes of data.
^C
--- 10.129.88.99 ping statistics ---
127 packets transmitted, 0 received, 100% packet loss, time 130452
```

4. Luego hacemos un NMAP para ver los servicios que usa la IP



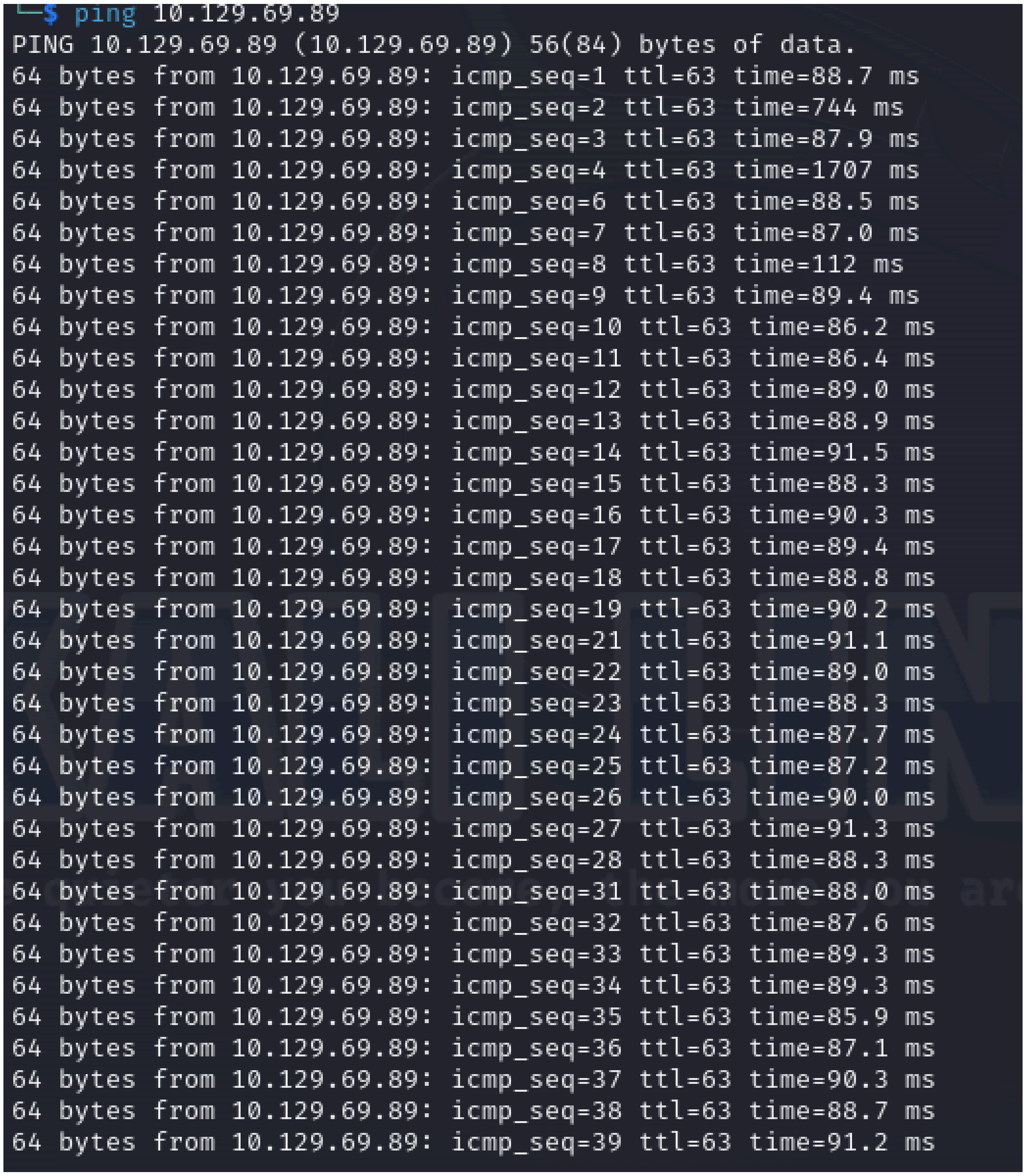
```
┌──(brahy㉿kali)-[~]
└─$ sudo nmap -sV 10.129.88.99
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-27 11:09 -05
Nmap scan report for 10.129.88.99
Host is up (0.014s latency).
All 1000 scanned ports on 10.129.88.99 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https:/
Nmap done: 1 IP address (1 host up) scanned in 9.06 seconds
```

Para esta IP no encontramos ninguna vulnerabilidad en los puertos por lo que debemos tomar otro camino

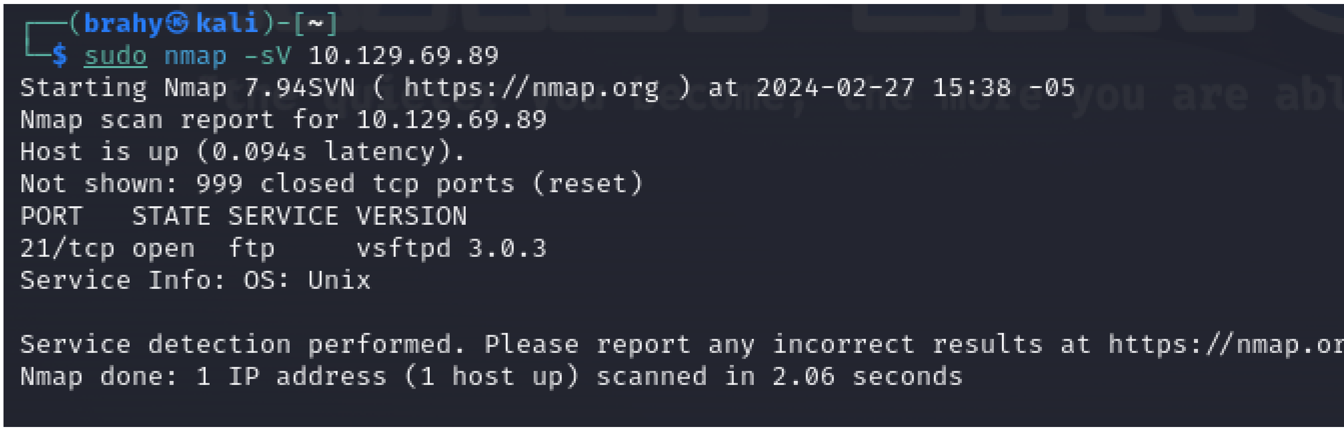
Segunda Máquina:

1. Ping a la ip 10.129.69.89



```
└─$ ping 10.129.69.89
PING 10.129.69.89 (10.129.69.89) 56(84) bytes of data.
64 bytes from 10.129.69.89: icmp_seq=1 ttl=63 time=88.7 ms
64 bytes from 10.129.69.89: icmp_seq=2 ttl=63 time=744 ms
64 bytes from 10.129.69.89: icmp_seq=3 ttl=63 time=87.9 ms
64 bytes from 10.129.69.89: icmp_seq=4 ttl=63 time=1707 ms
64 bytes from 10.129.69.89: icmp_seq=6 ttl=63 time=88.5 ms
64 bytes from 10.129.69.89: icmp_seq=7 ttl=63 time=87.0 ms
64 bytes from 10.129.69.89: icmp_seq=8 ttl=63 time=112 ms
64 bytes from 10.129.69.89: icmp_seq=9 ttl=63 time=89.4 ms
64 bytes from 10.129.69.89: icmp_seq=10 ttl=63 time=86.2 ms
64 bytes from 10.129.69.89: icmp_seq=11 ttl=63 time=86.4 ms
64 bytes from 10.129.69.89: icmp_seq=12 ttl=63 time=89.0 ms
64 bytes from 10.129.69.89: icmp_seq=13 ttl=63 time=88.9 ms
64 bytes from 10.129.69.89: icmp_seq=14 ttl=63 time=91.5 ms
64 bytes from 10.129.69.89: icmp_seq=15 ttl=63 time=88.3 ms
64 bytes from 10.129.69.89: icmp_seq=16 ttl=63 time=90.3 ms
64 bytes from 10.129.69.89: icmp_seq=17 ttl=63 time=89.4 ms
64 bytes from 10.129.69.89: icmp_seq=18 ttl=63 time=88.8 ms
64 bytes from 10.129.69.89: icmp_seq=19 ttl=63 time=90.2 ms
64 bytes from 10.129.69.89: icmp_seq=21 ttl=63 time=91.1 ms
64 bytes from 10.129.69.89: icmp_seq=22 ttl=63 time=89.0 ms
64 bytes from 10.129.69.89: icmp_seq=23 ttl=63 time=88.3 ms
64 bytes from 10.129.69.89: icmp_seq=24 ttl=63 time=87.7 ms
64 bytes from 10.129.69.89: icmp_seq=25 ttl=63 time=87.2 ms
64 bytes from 10.129.69.89: icmp_seq=26 ttl=63 time=90.0 ms
64 bytes from 10.129.69.89: icmp_seq=27 ttl=63 time=91.3 ms
64 bytes from 10.129.69.89: icmp_seq=28 ttl=63 time=88.3 ms
64 bytes from 10.129.69.89: icmp_seq=31 ttl=63 time=88.0 ms
64 bytes from 10.129.69.89: icmp_seq=32 ttl=63 time=87.6 ms
64 bytes from 10.129.69.89: icmp_seq=33 ttl=63 time=89.3 ms
64 bytes from 10.129.69.89: icmp_seq=34 ttl=63 time=89.3 ms
64 bytes from 10.129.69.89: icmp_seq=35 ttl=63 time=85.9 ms
64 bytes from 10.129.69.89: icmp_seq=36 ttl=63 time=87.1 ms
64 bytes from 10.129.69.89: icmp_seq=37 ttl=63 time=90.3 ms
64 bytes from 10.129.69.89: icmp_seq=38 ttl=63 time=88.7 ms
64 bytes from 10.129.69.89: icmp_seq=39 ttl=63 time=91.2 ms
```

2. Nmap a la IP

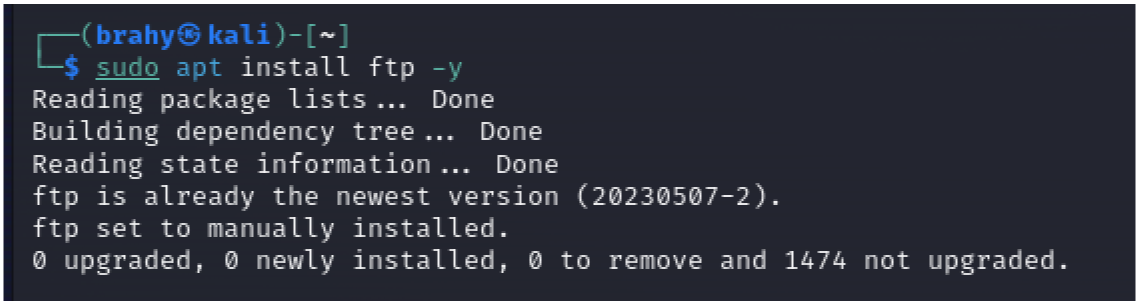


```
┌──(brahy㉿kali)-[~]
└─$ sudo nmap -sV 10.129.69.89
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-27 15:38 -05
Nmap scan report for 10.129.69.89
Host is up (0.094s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.or
Nmap done: 1 IP address (1 host up) scanned in 2.06 seconds
```

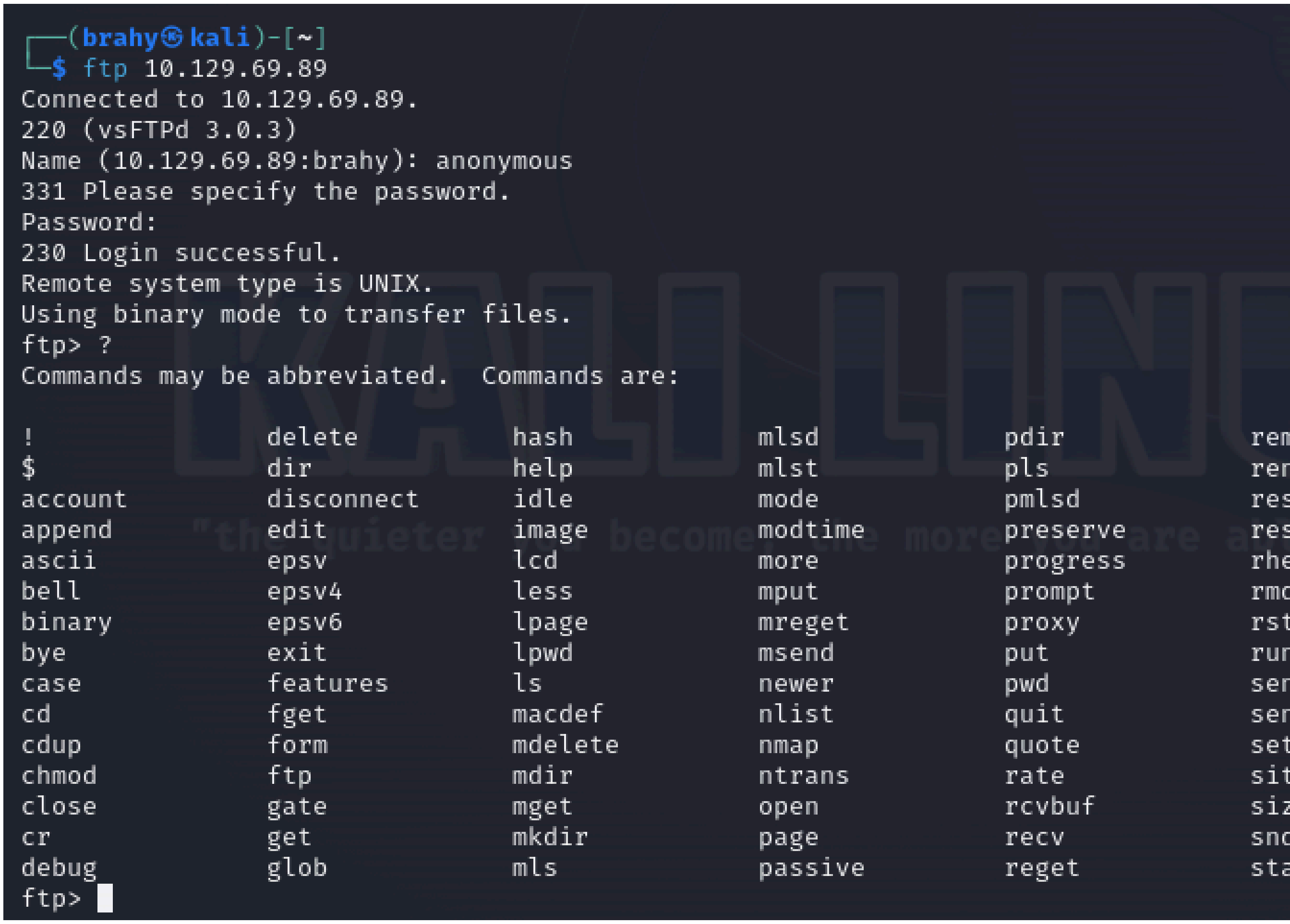
donde encontramos que el puerto 21/tcp esta abierto con el servicio de vsftpd 3.0.3

3. hacemos la instalacion de el servicio



```
┌──(brahy㉿kali)-[~]
└─$ sudo apt install ftp -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
ftp is already the newest version (20230507-2).
ftp set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 1474 not upgraded.
```

4. Y usamos el servicio para intentar ingresar por el puerto abierto de forma anónima



```
┌──(brahy㉿kali)-[~]
└─$ ftp 10.129.69.89
Connected to 10.129.69.89.
220 (vsFTPd 3.0.3)
Name (10.129.69.89:brahy): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ?
Commands may be abbreviated.  Commands are:

!               delete          hash            mlsd            pdir            rem
$               dir             help            mlst            pls             ren
account         disconnect      idle            mode            pmlsd           res
append          edit            image           modtime         preserve        res
ascii           epsv            lcd             more            progress        rhe
bell            epsv4           less            mput            prompt          rmd
binary          epsv6           lpage           mreget          proxy           rst
bye             exit            lpwd            msend           put             run
case            features        ls              newer           pwd             sen
cd              fget            macdef          nlist           quit            sen
cdup            form            mdelete         nmap            quote           set
chmod           ftp             mdir            ntrans          rate            sit
close           gate            mget            open            rcvbuf          siz
cr              get             mkdir           page            recv            snd
debug           glob            mls             passive         reget           sta
ftp> 
```

Donde ya podemos acceder a sus documentos ya que conocemos varios de estas sintaxis en nuestra terminal