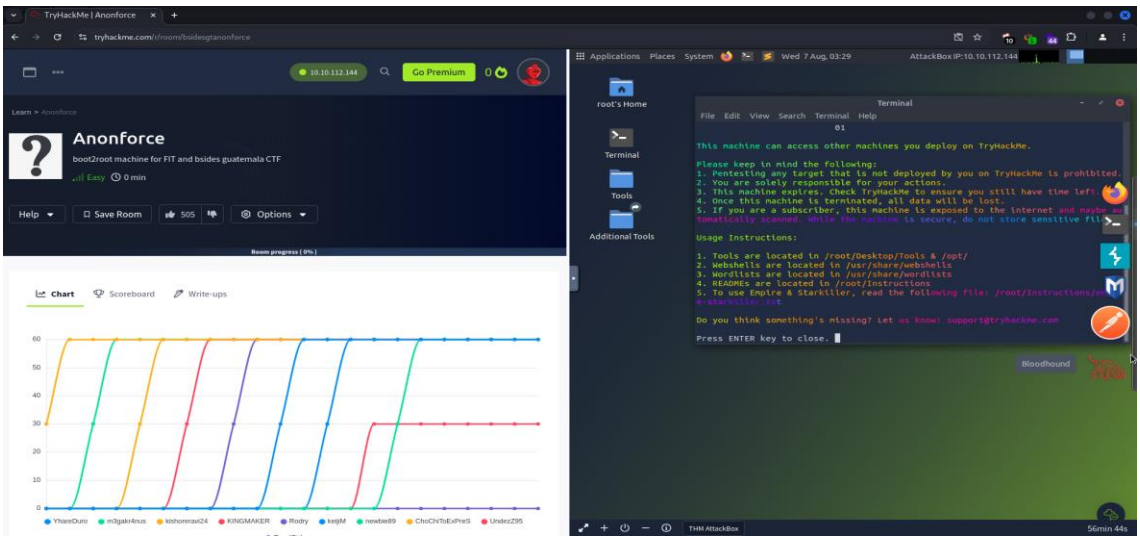
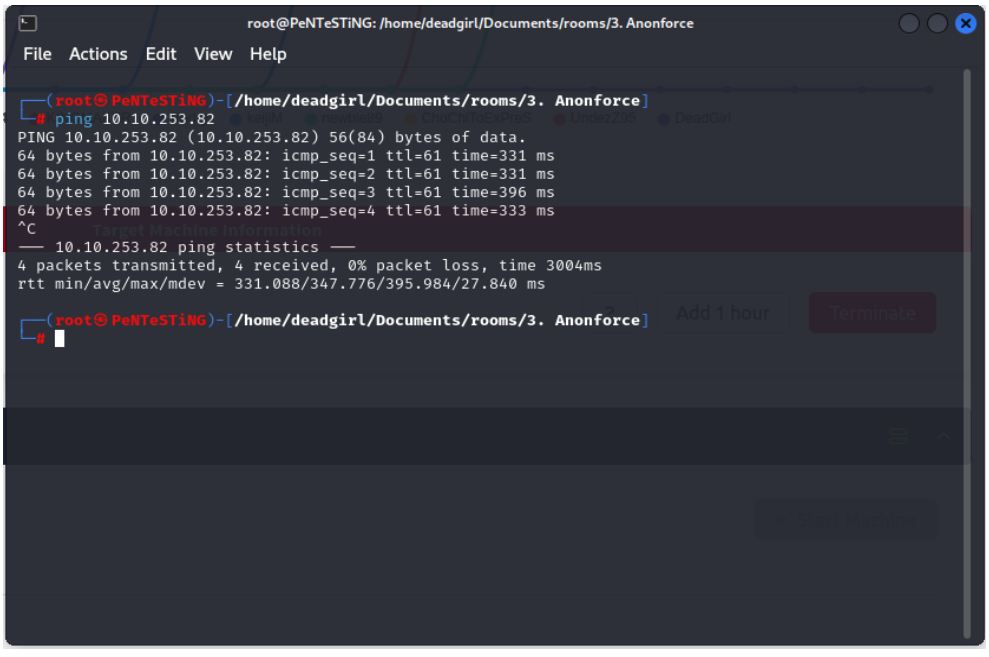
Anonforce

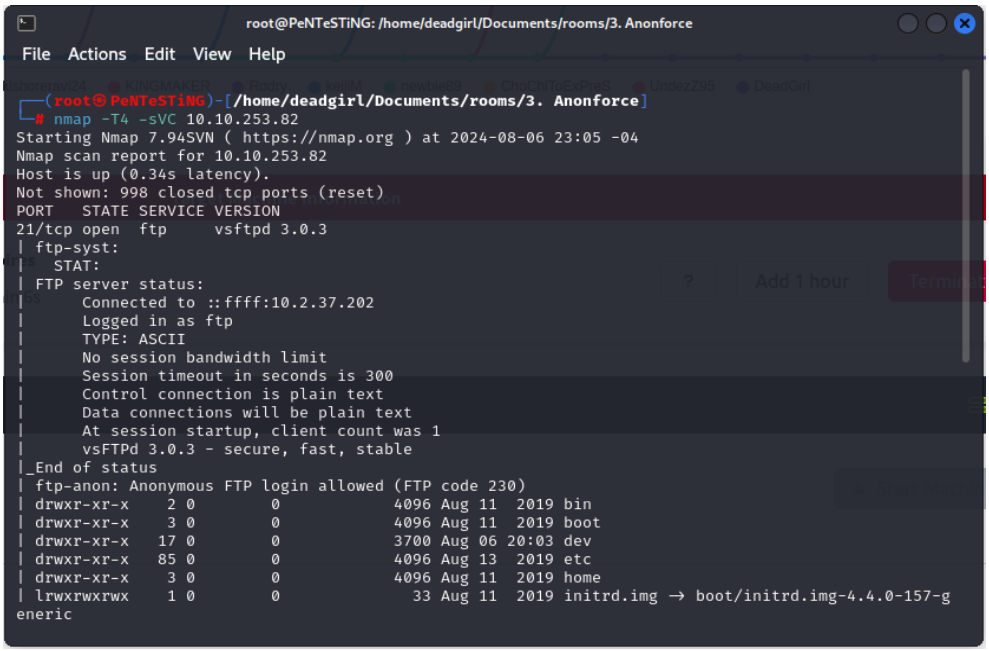
Anonforce es una maquina bastante sencilla que no toma entre 5 - 10 minutos el poder resolverla y el proposito es poder obtener información de claves privadas.

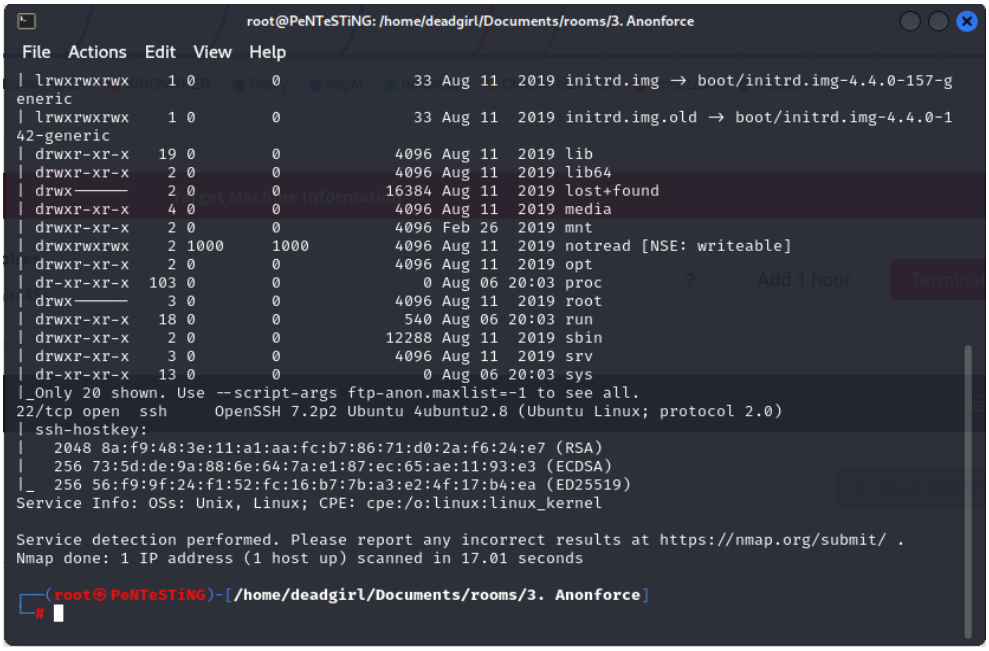


Lo primero es realizar ping hacia la máquina para corroborar que tenemos respuesta ICMP, con el comando ***ping 10.10.253.82*** (más adelante esta IP cambia… XD se me había acabado el tiempo XD)

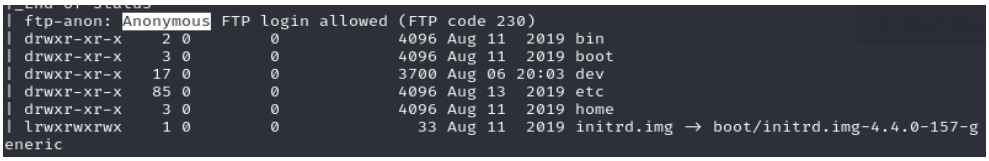


Luego con el comando ***nmap –T4 –sVC 10.10.253.82*** veras los puertos abierto. Hay 2 servicios en ejecución: FTP y SSH.

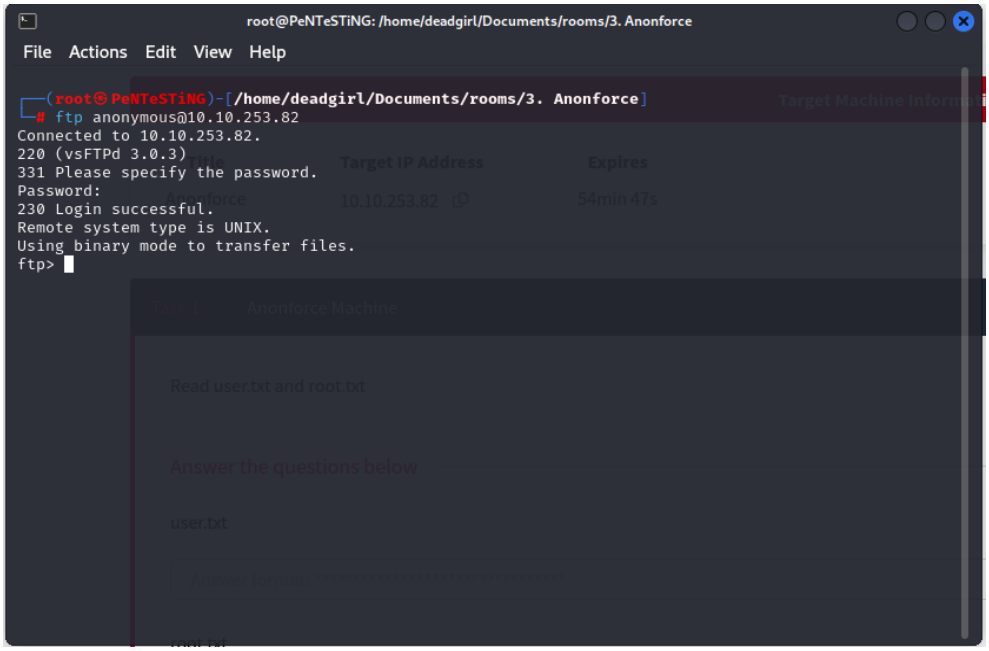




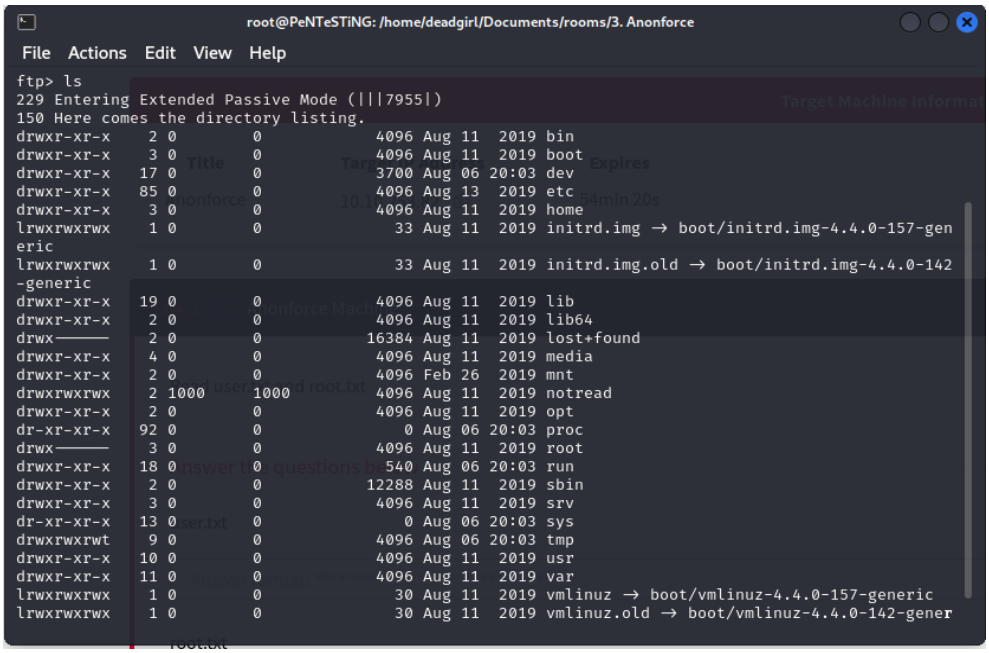
Como se logra observar, no tan solo ha detectado el puerto 21 FTP abierto, sino que también ha descubierto un usuario ***Anonymous***

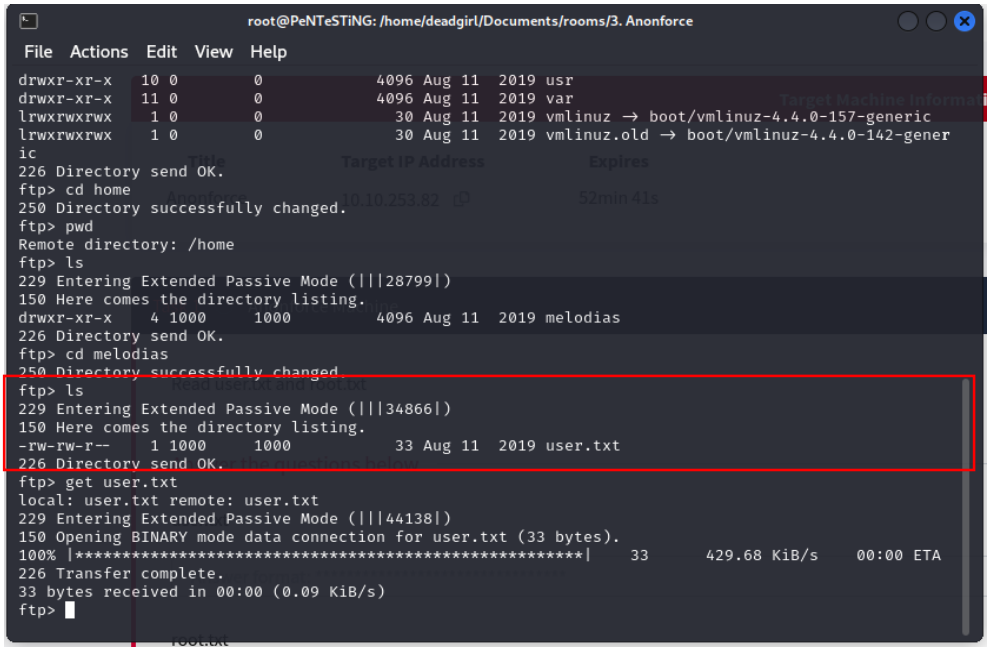


Primero, iniciar sesión en FTP como Anonymous, aquí solicitara una Password, en mi caso solo presioné enter y pude ingresar vía Telnet.

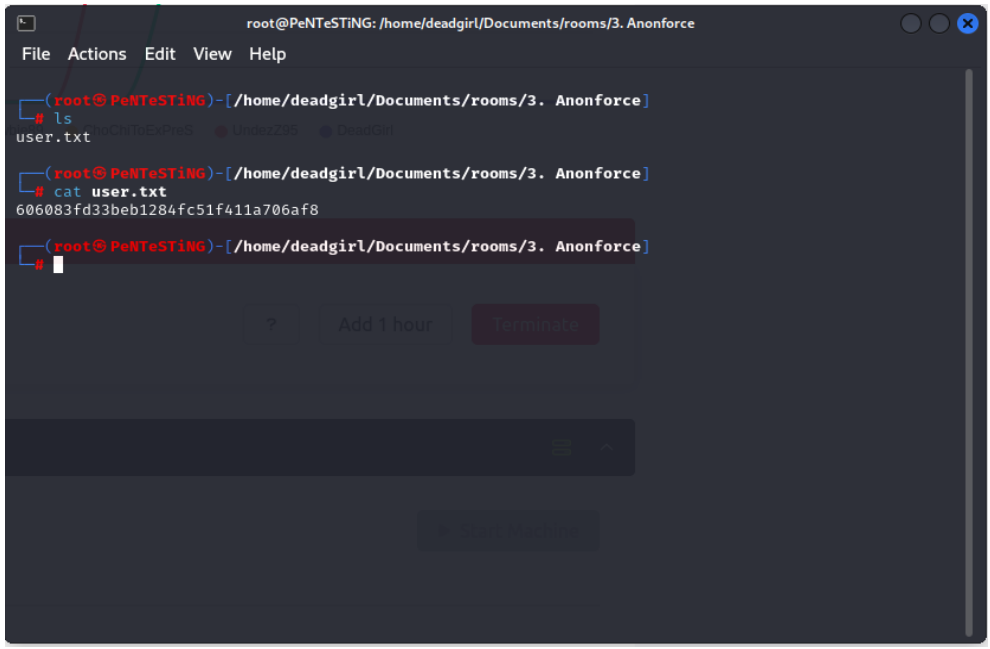


Luego de un rato, comencé a moverme por los directorios para encontrar archivos valiosos. Después de un rato, encontré la primera bandera: ***user.txt***

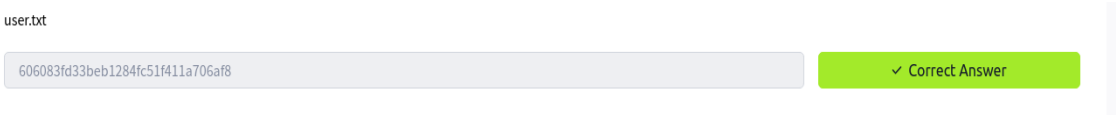




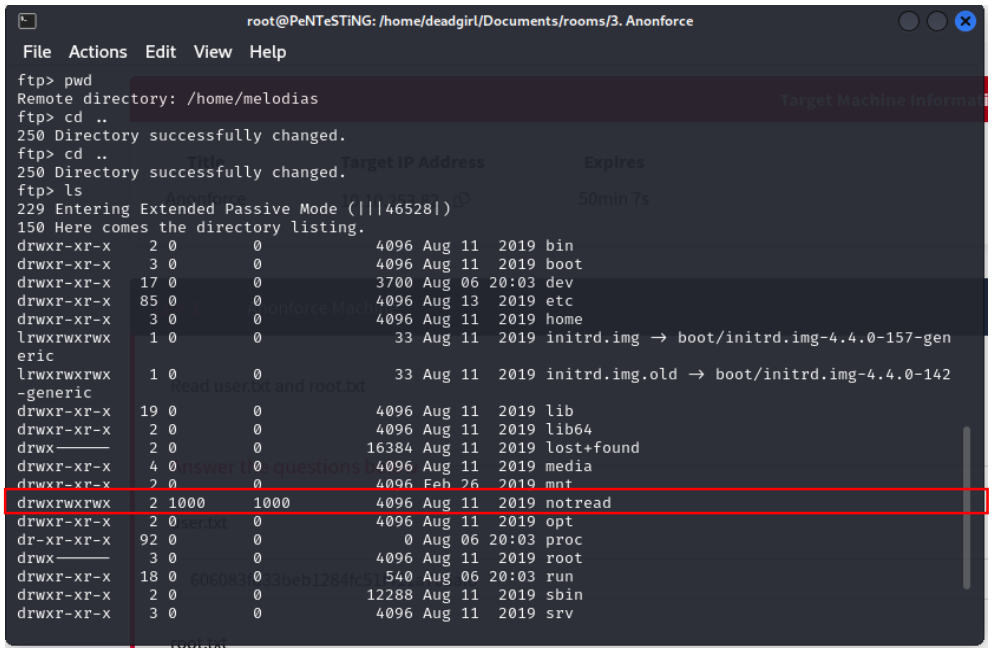
El archivo user.txt lo he copiado a mi directorio (he creado una carpeta que contiene lo archivos que iré descargando conforme vaya avanzando en la resolución de la máquina) y con el comando ***cat user.txt*** se obtiene la primera bandera.



Primera bandera

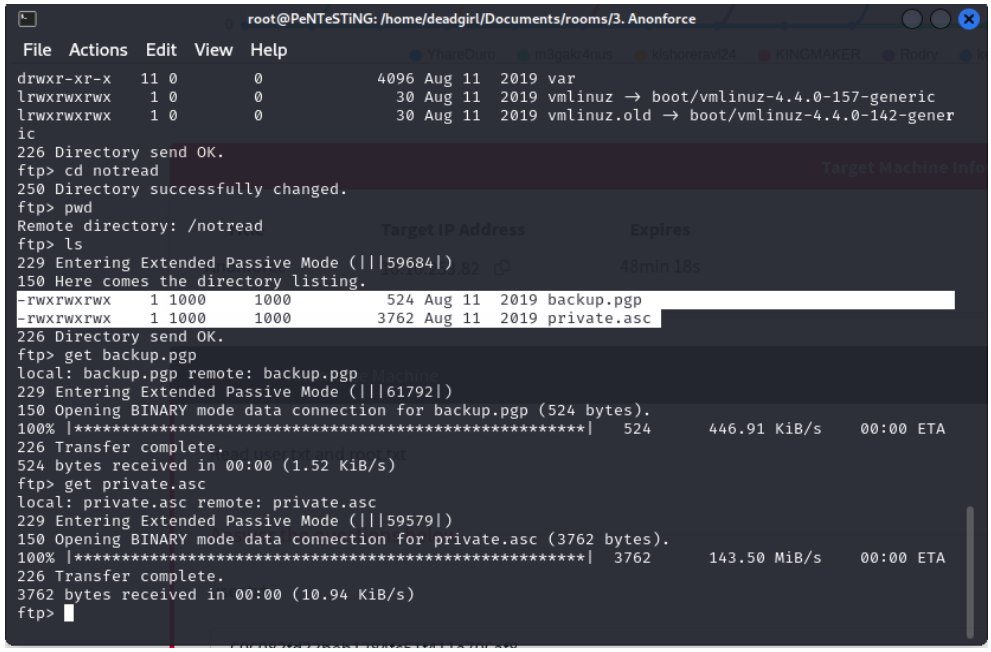


Regreso al directorio raíz y aquí observo otro directorio con el nombre ***notread***.



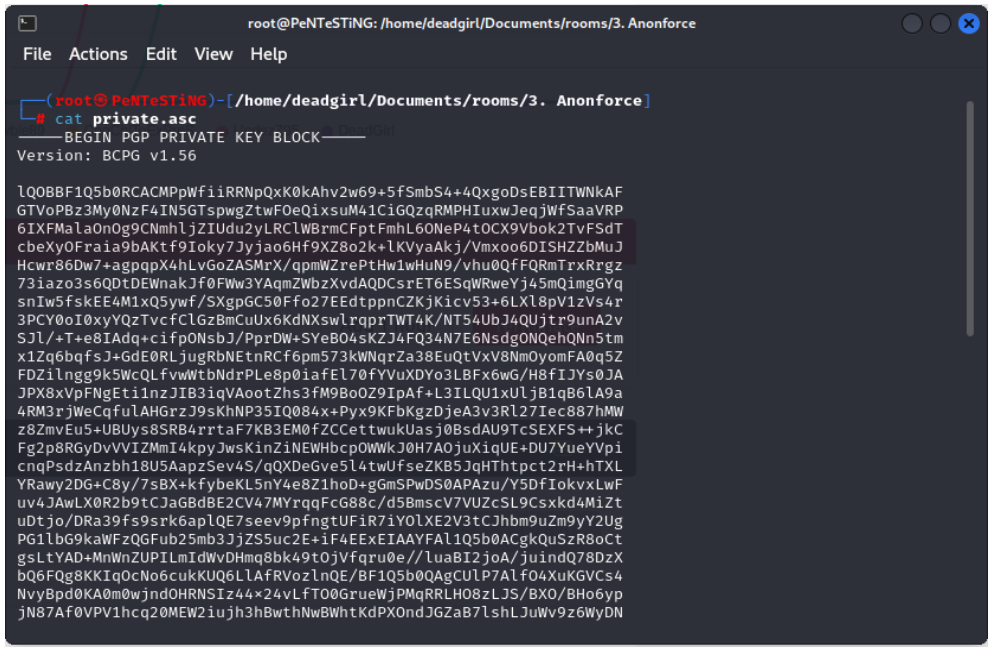
Con el comando ***cd notread*** ingresar a dicho directorio y posterior con el comando ***ls*** se observa 2 archivos:

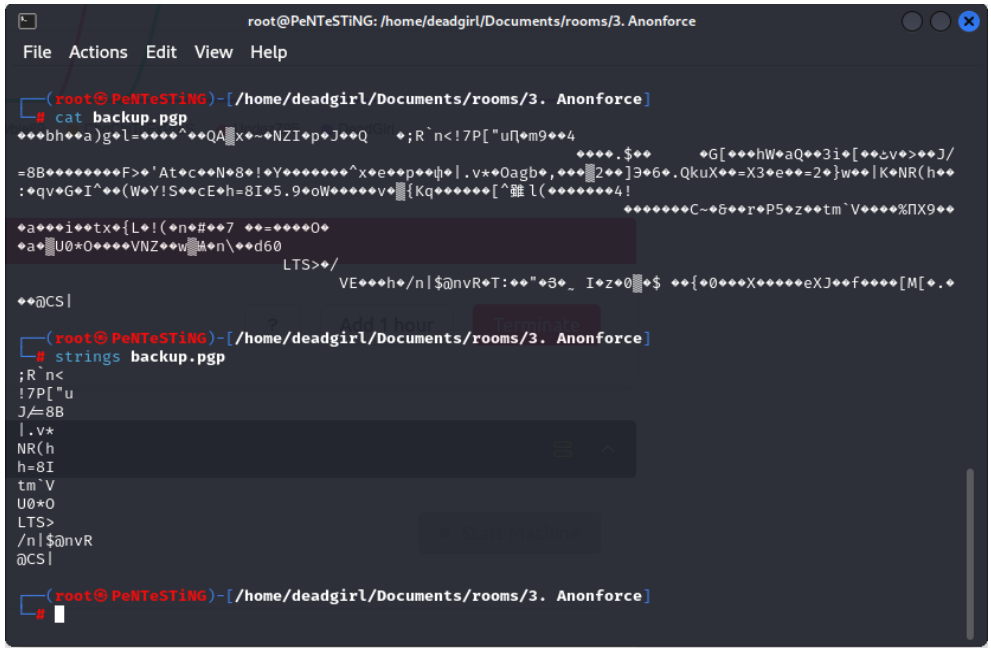
- ***backup.pgp***
- ***private.asc***



Con el comando ***get*** descargar ambos archivos al directorio de preferencia (en mi caso he creado un directorio exclusivo para la resolución de la máquina)

Luego con el comando ***cat private.asc*** y el comando ***cat backup.gpg*** se observa el bloque de claves cifrados, al igual que con el comando ***strings*** se intenta observar para el archivo backup.pgp la clave cifrada, pero sigue siendo ilegible.

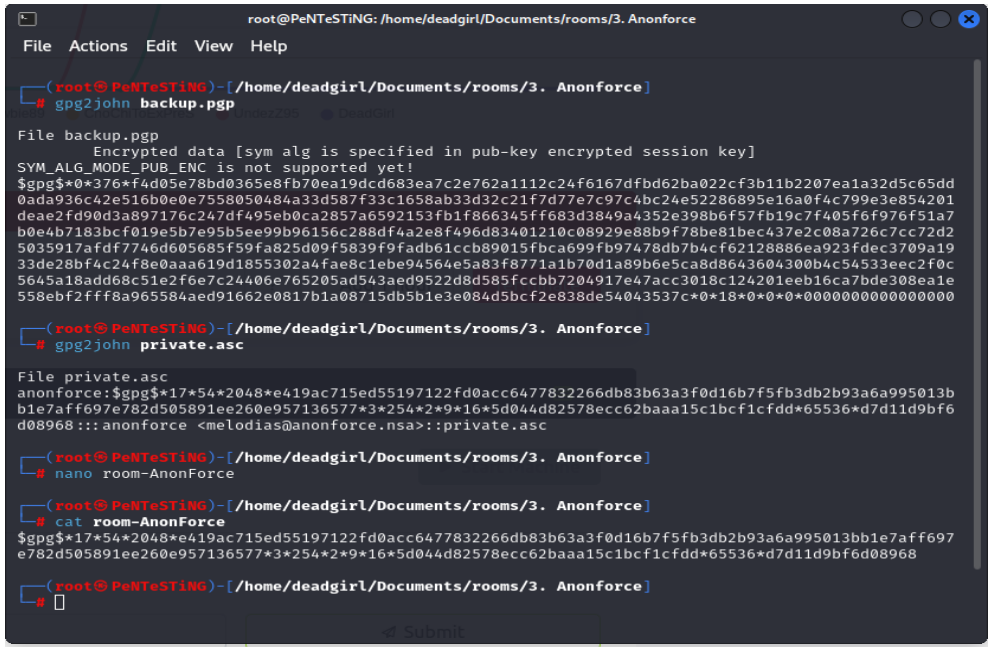




Como se mencionó anteriormente, con los comandos cat y strings las claves privadas son ilegibles, con el siguiente comando ***gpg2john backup.pgp*** y el comando ***gpg2john private.asc*** se extraerá y transformará las contraseñas cifradas en archivos de clave GPG legible.

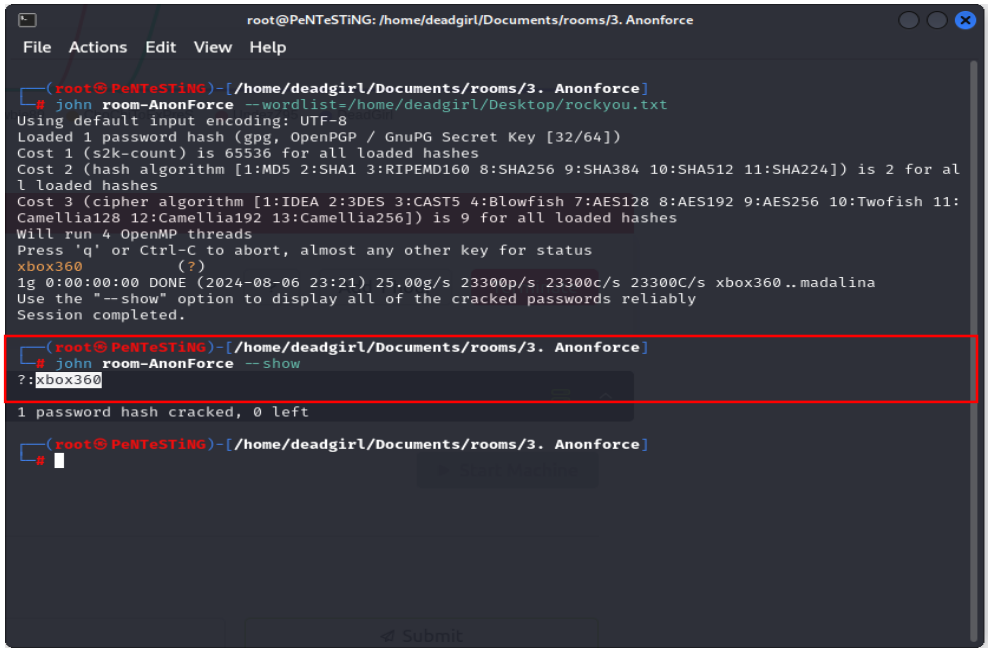
NOTA: GPG por su sigla en inglés (GNU Privacy Guard) es una herramienta de cifrado y firma digital que se utiliza para asegurar la comunicación y los datos mediante criptografía de clave pública

En mi caso cree un archivo de texto con el comando ***nano room-Anonforce*** el cual he guardado la clave cifrada del usuario anonforce, ya con el comando **cat room-Anonforce** se observa y corrobora que dicha clave ha sido guardada.

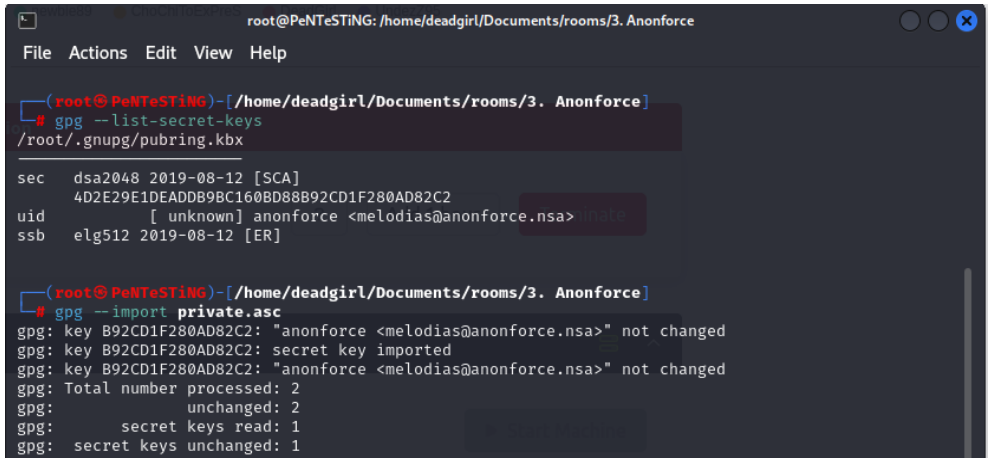


Primero, use gpg2john para cambiar la clave privada al formato que John pueda leer y luego con el comando ***John room-Anonforce --wordlist=/home/deadgirl/Desktop/rockyou.txt*** descifrar la contraseña cifrada.

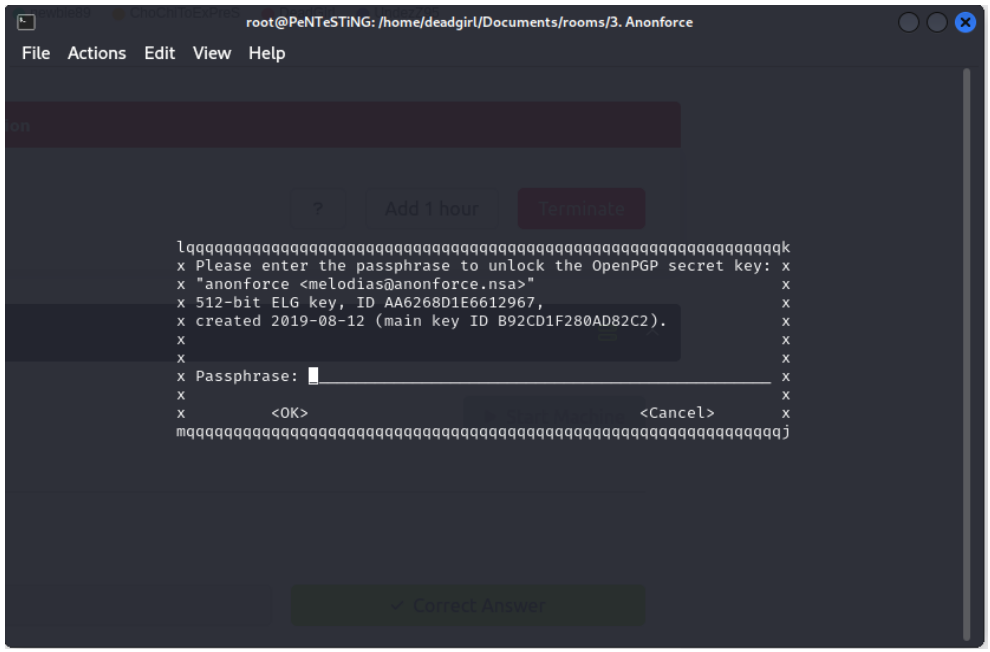
Con el comando ***John room-Anonforce --show*** verificar la password descifrada.



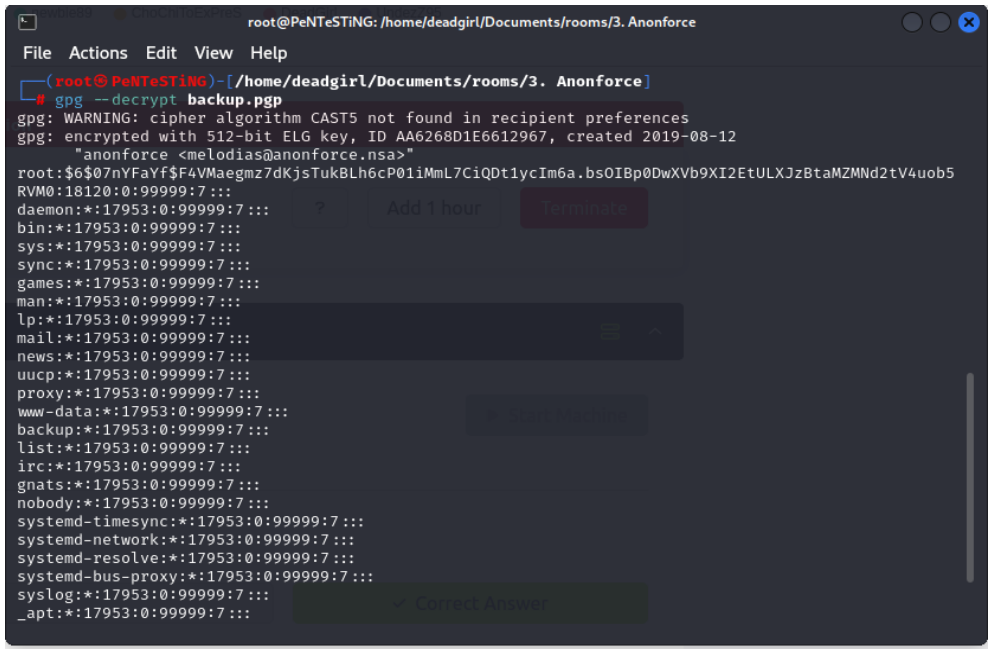
Con el comando ***gpg –list-secret-keys*** en mi caso quise listar las claves secretas y con el comando ***gpg --import private.asc*** se importa la clave privada.



Con el comando ***gpg --decrypt backup.pgp*** importar dicha clave cifrada con la password que se ha descubierto con el comando John.

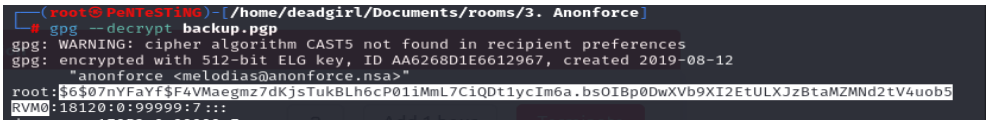


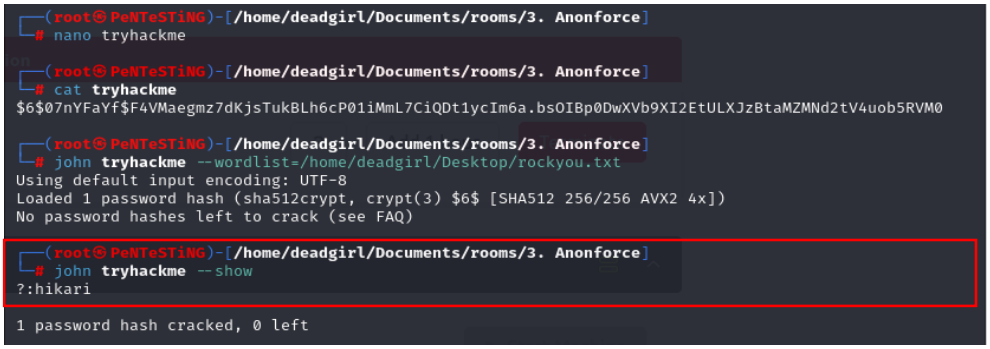
Ahora se ha importado la clave. Se ha descifrado el archivo de copia de seguridad.



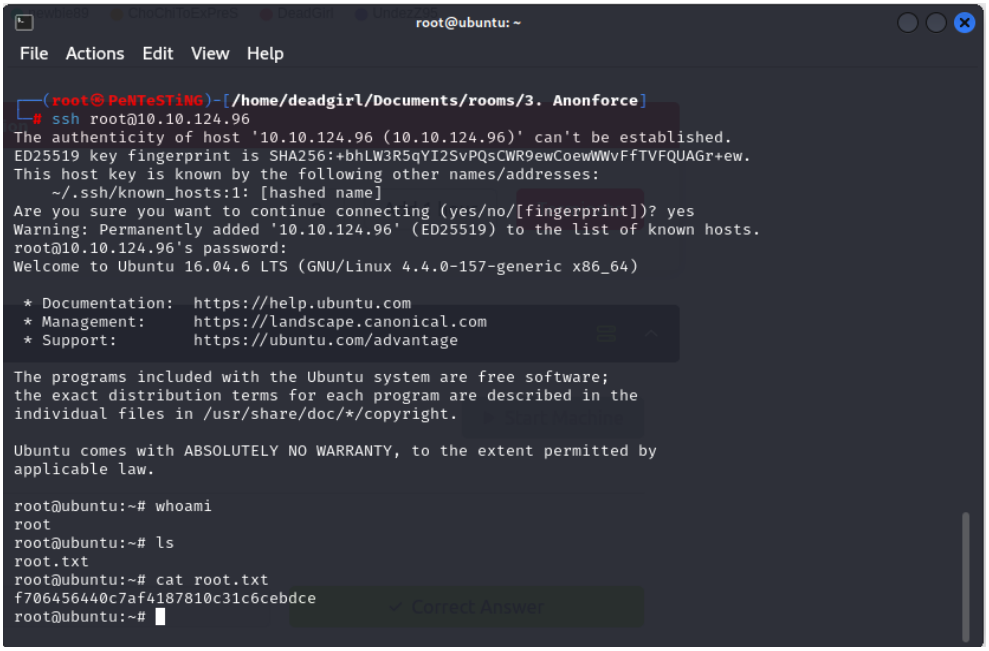
Lo mismo que se realizó anteriormente, he creado otro archivo, pero he copiado la clave cifrada del usuario ***root*** y he creado un archivo de texto con el comando y nombre ***nano tryhackme*** y con el comando ***cat tryhackme*** se muestra el contenido del archivo.

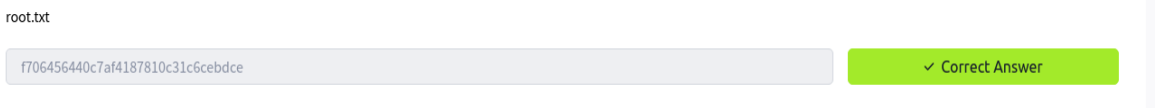
Volver a repetir el mismo procedimiento de descifrar la password con el comando ***john tryhackme --wordlist=/home/deadgirl/Desktop/rockyou.txt*** y con el comando ***john tryhackme --show*** se obtiene el comando ***hokari***

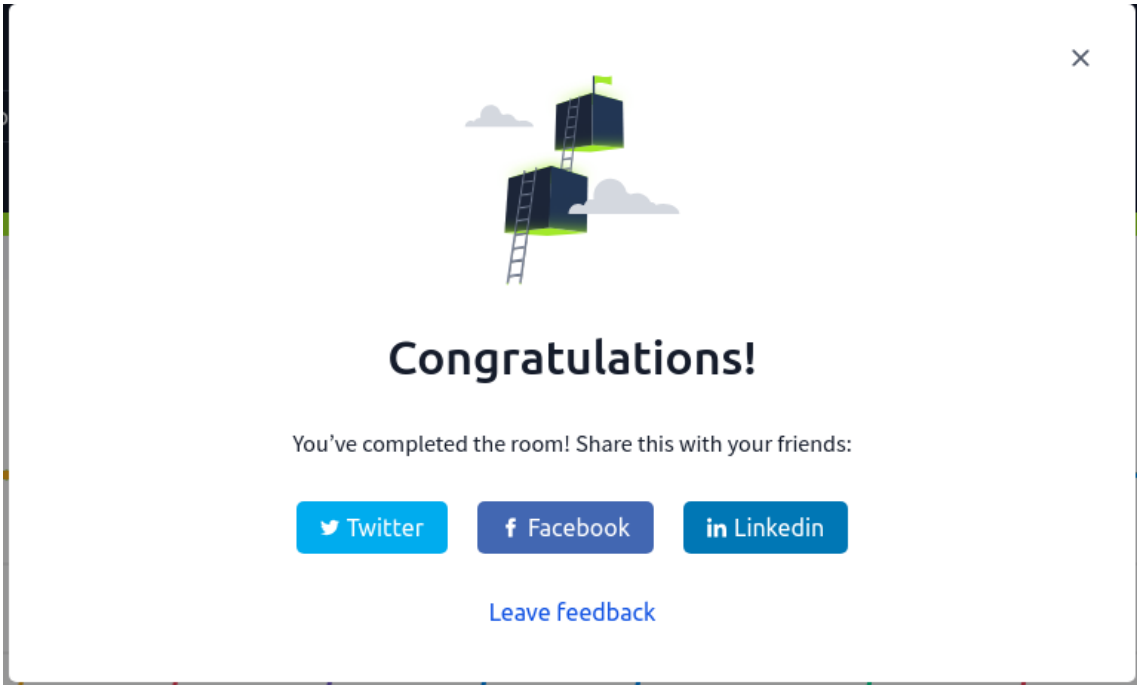




Ahora tengo la contraseña de root. Consigue la bandera final.






Congratulations!
You've completed the room! Share this with your friends:
Twitter
Facebook
Linkedin
Leave feedback