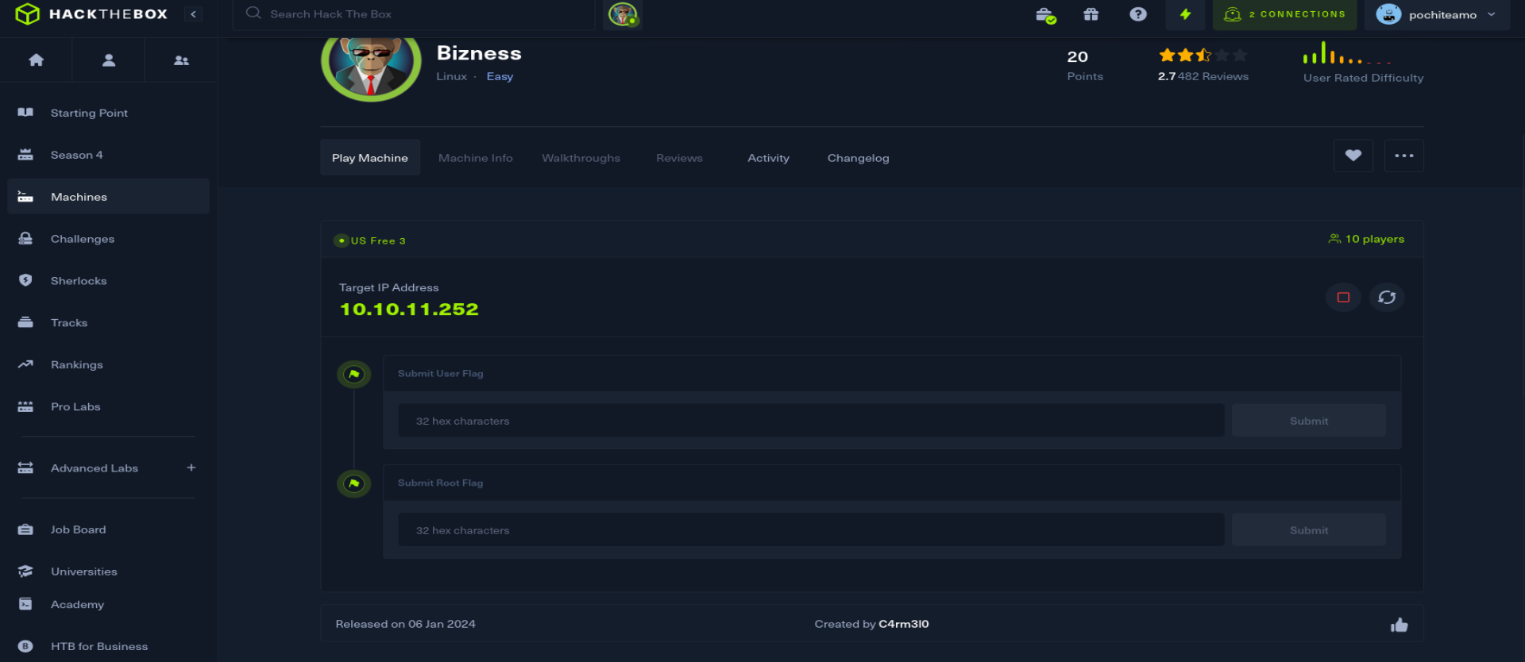
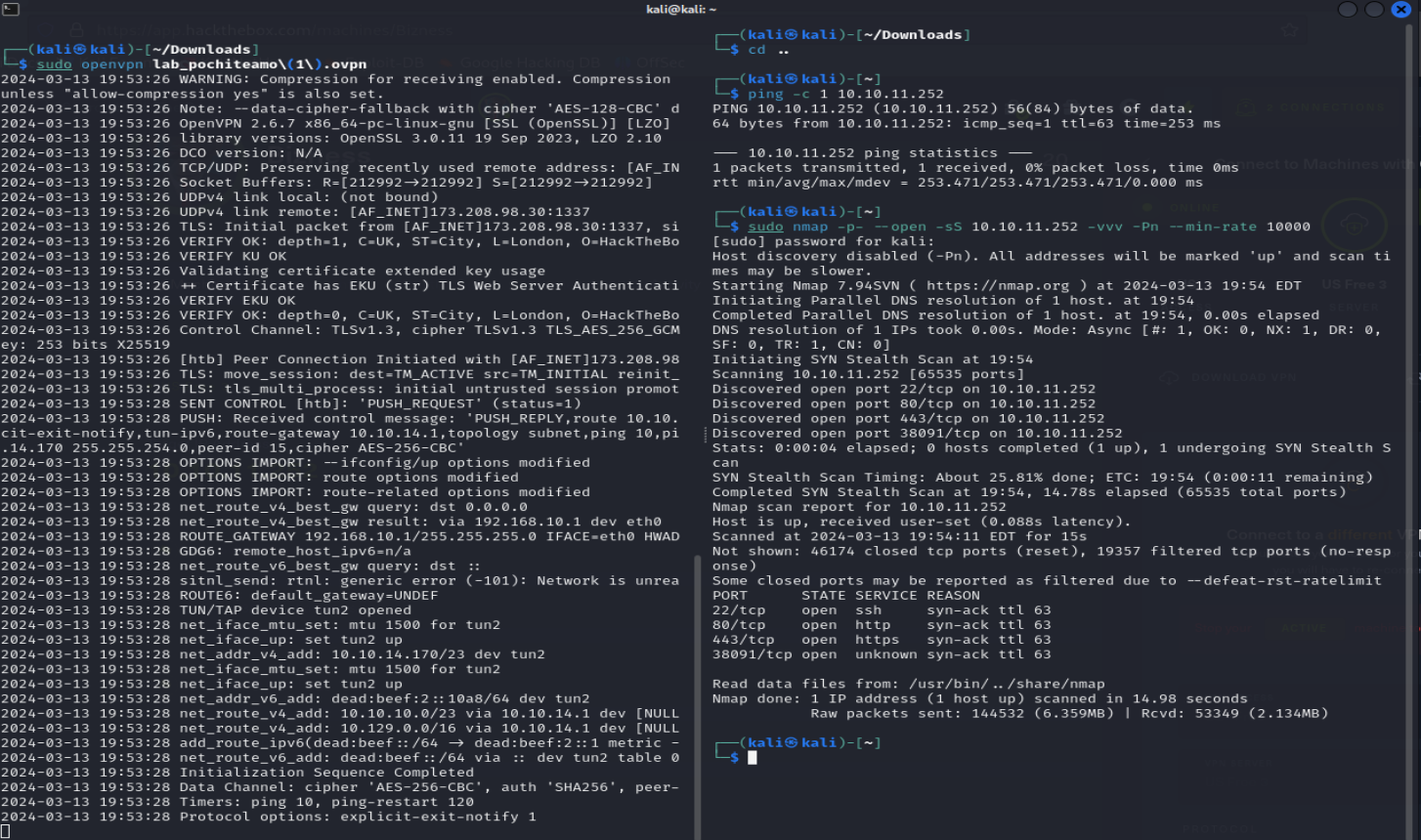
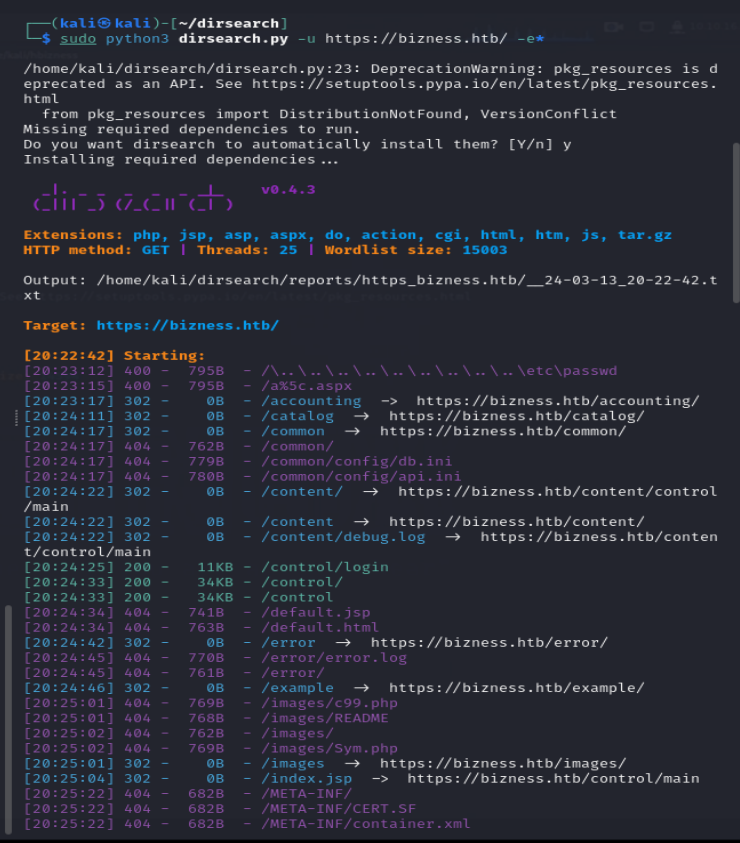
Bizness

1. Elegimos la maquina del hackthebox que en este caso es Bizness
2. Hacemos ping y el nmap

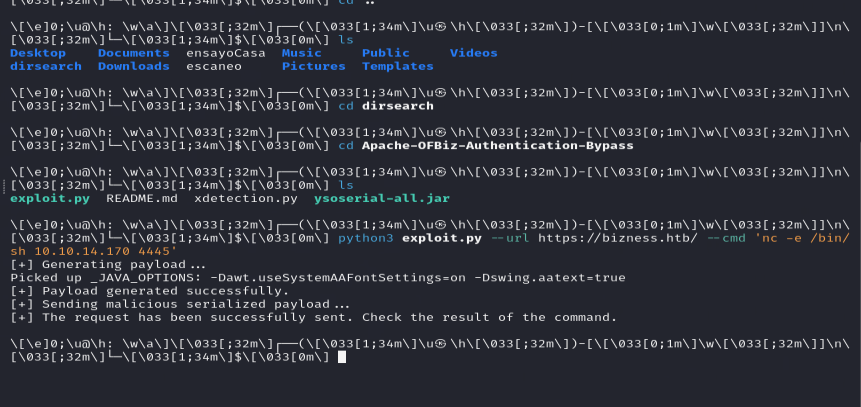


Ejecutamos el comando de la imagen anterior que es ese nmap, para ver exactamente los puertos que necesitamos, específicamente escaneo de versiones, escaneo de scripts predeterminados y la detección de la versión del software

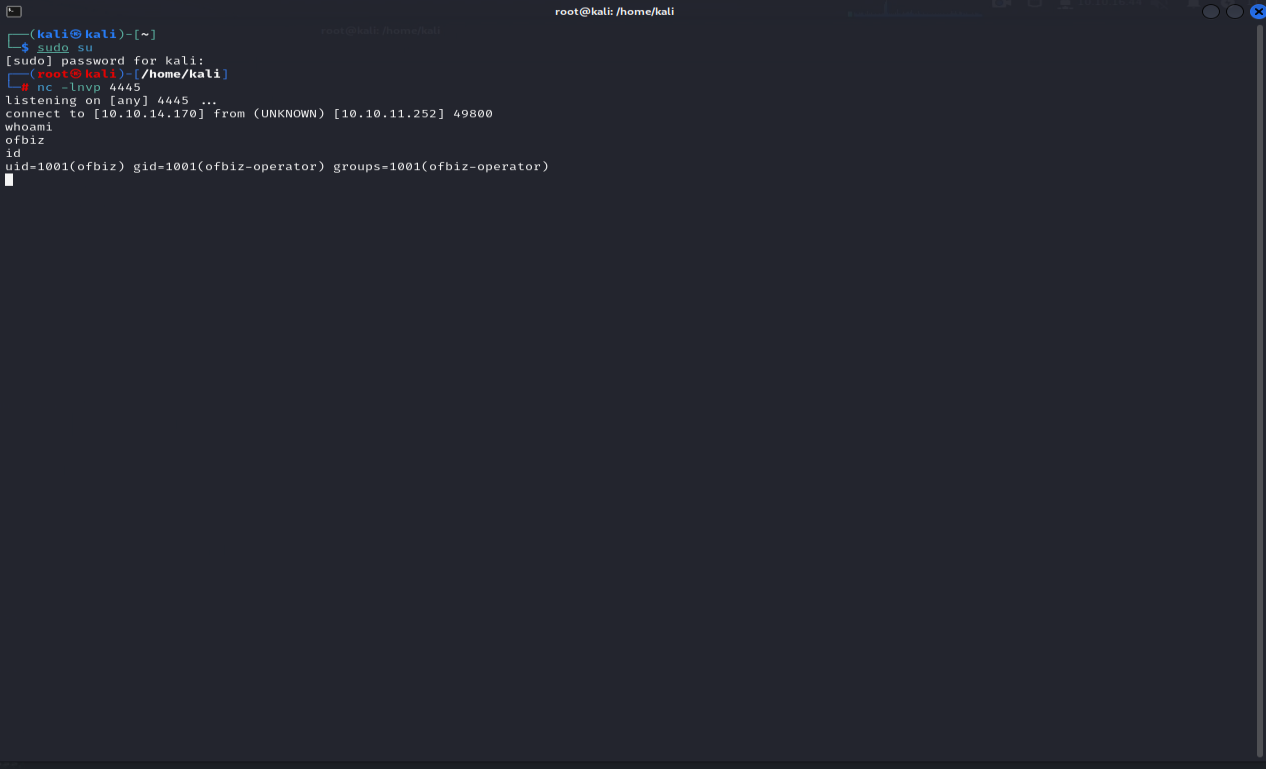
1. El comando busca directorios y archivos en el sitio web https://bizness.htb/



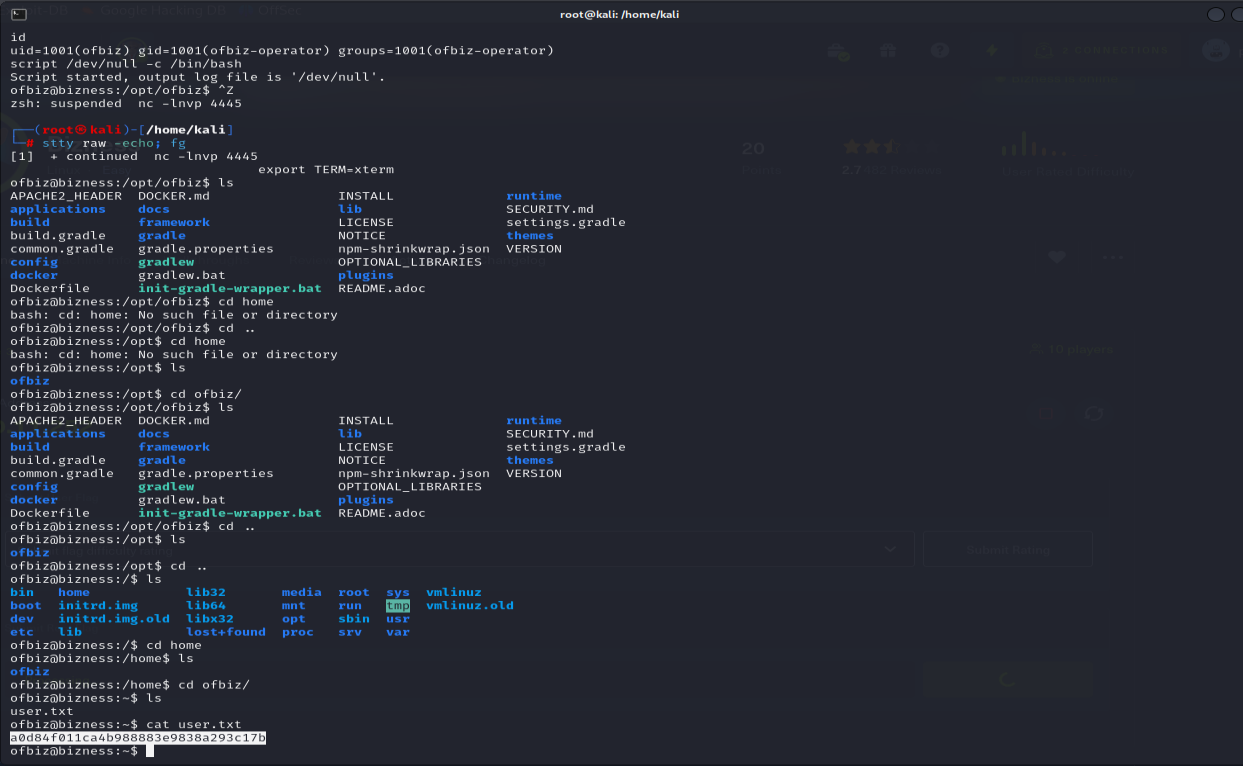
1. Corremos el script



* Ponemos a escuchar desde otro puerto para al correr el script podamos acceder.



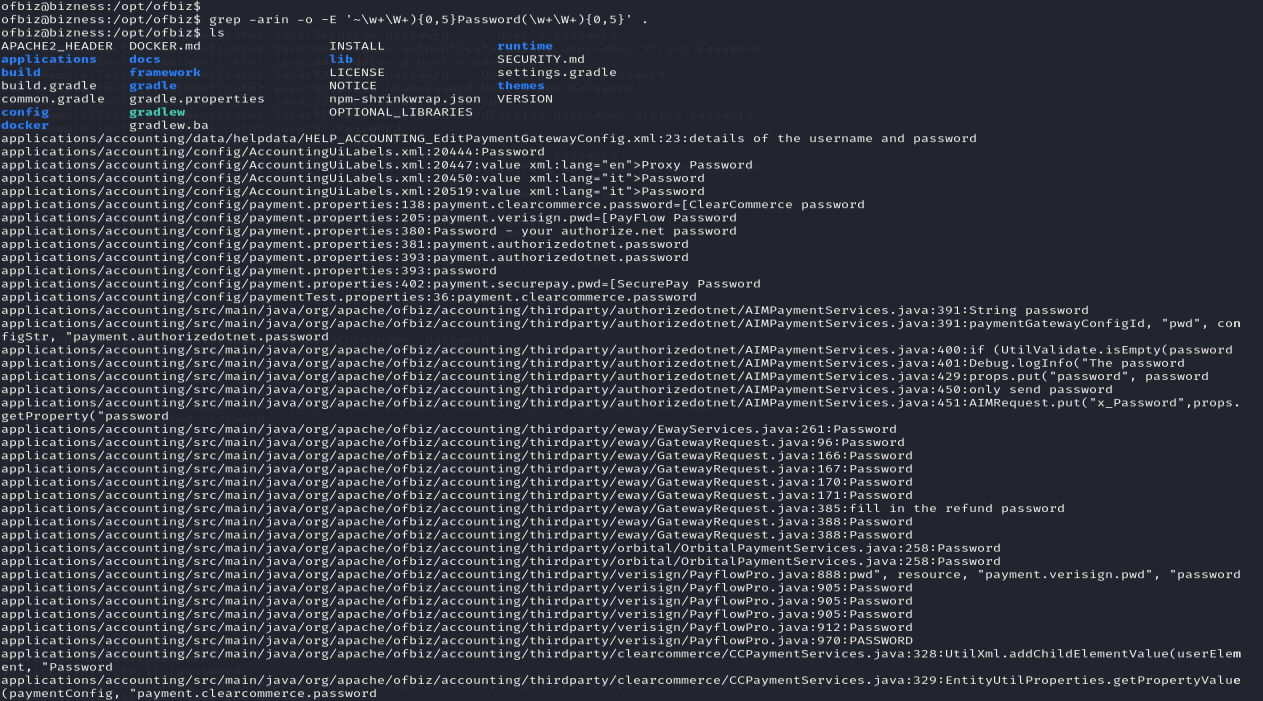
1. Ya con esto, ingresamos.. hacemos los comandos de whoami y el id, navegamos hasta encontrar el archivo user.txt y encontramos la primera bandera



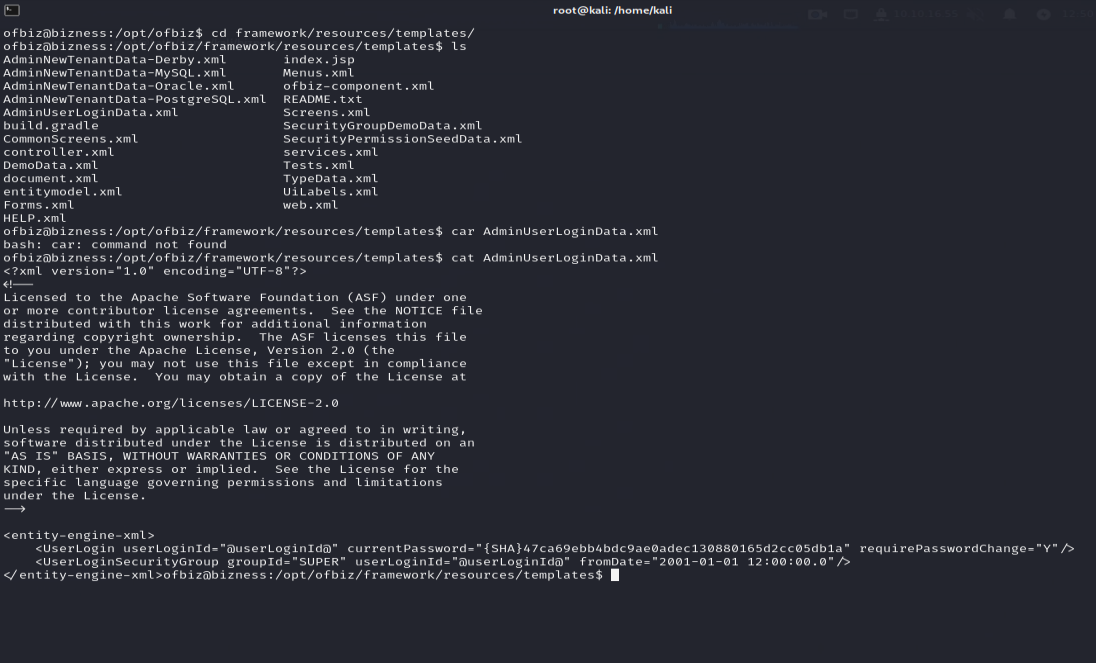
Luego..

Usamos un script para este directorio que vemos en las imágenes, para encontrar archivos con la palabra password

grep -arin -o -E '(\w+\W+){0,5}Password(\w+\W+){0,5}'

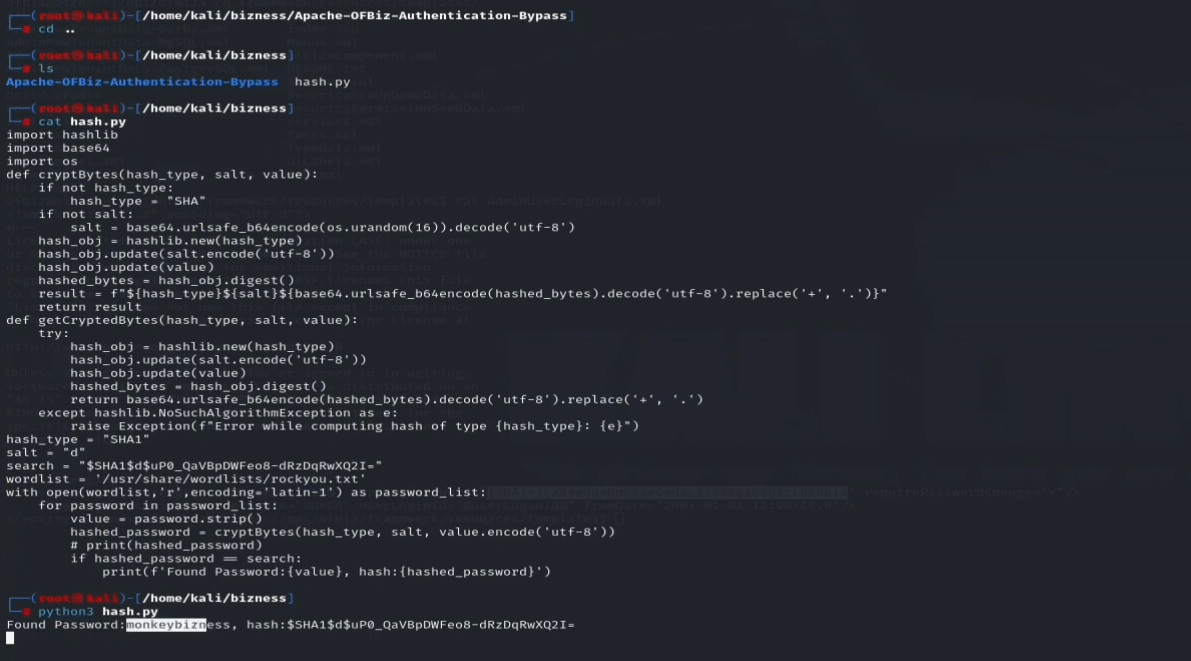


1. Encontramos una ruta y un archivo que nos importa

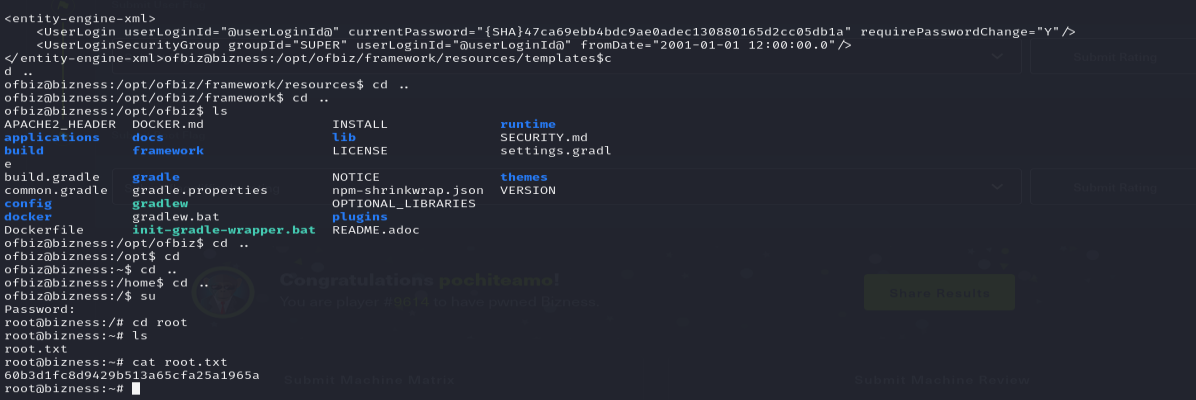


Vamos a desencriptarla

Con un archivo Python la desencriptamos y la clave que obtenemos de aquí es: monkeybizness



1. Ya con acceso al root vamos a obtener la bandera, encontramos el archivo root.txt



1. Finalizamos, hemos encontrado las dos banderas.. y completado el hackthebox

