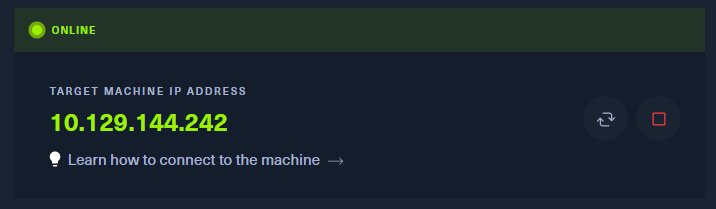
ANALISIS MAQUINA VIRTUAL REDEEMER

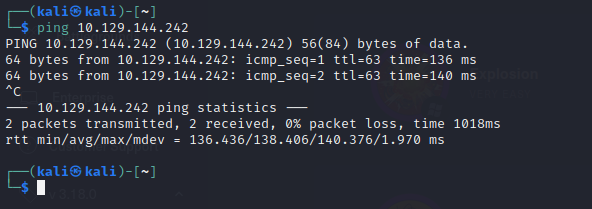
Dificultad: Facil

Etiqueta: Enumeración, Penetración, Attacks/Anonymous, Redis

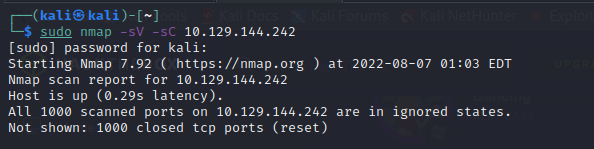
IP Maquina



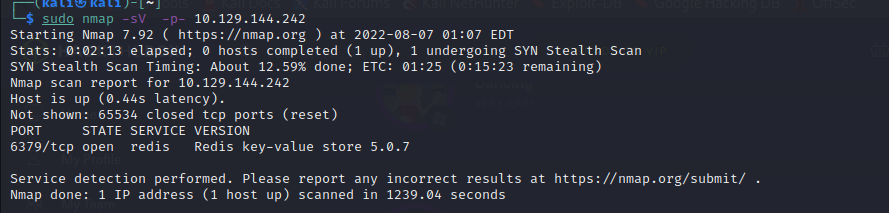
Realizamos ping para ver si tenemos conexión



Escaneamos para ver los puertos y servicios



Al no tener ningún puerto tenemos que colocar todos los puertos en general



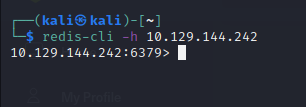
Solo un puerto está abierto en la máquina de destino, es decir, el puerto 6379 que es ejecutando un servidor Redis.

Redis (REmote DIctionary Server) es un almacén de datos clave-valor NoSQL avanzado de código abierto que se utiliza como base de datos, caché y agente de mensajes. Los datos se almacenan en un formato de diccionario que tiene pares clave-valor. Está normalmente se utiliza para el almacenamiento a corto plazo de datos que necesitan una recuperación rápida. Redis hace copias de seguridad de datos en discos duros para dar consistencia

Ahora, para poder interactuar de forma remota con el servidor Redis, necesitamos descargar la utilidad redis-cli. Eso se puede descargar usando el siguiente comando:

sudo apt install redis-tools

Una vez instalado vamos a la terminal para conectarnos con el servidor redist con el comando

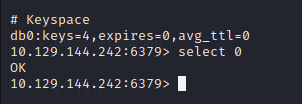


La conexión es exitosa

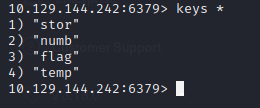
Ahora Uno de los comandos básicos de enumeración de Redis es info, que devuelve información y estadísticas sobre el servidor Redis.

La sección de espacio de claves proporciona estadísticas sobre el diccionario principal de cada base de datos. Las estadísticas incluyen la número de claves y el número de claves con vencimiento.

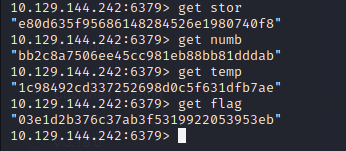
En nuestro caso, en la sección Keyspace, podemos ver que solo existe una base de datos con el índice 0. Seleccionemos esta base de datos lógica de Redis usando el comando select seguido del número de índice de la base de datos que necesita ser seleccionada:



Además, podemos listar todas las claves presentes en la base de datos usando el comando: keys \*



Finalmente, podemos ver los valores almacenados para una clave correspondiente usando el comando get seguido del nota clave:



Bandera que nos interesa es el flag: 03e1d2b376c37ab3f5319922053953eb