# Remote buster/mapper

- José Catalán Fuentes 201551010 - 5

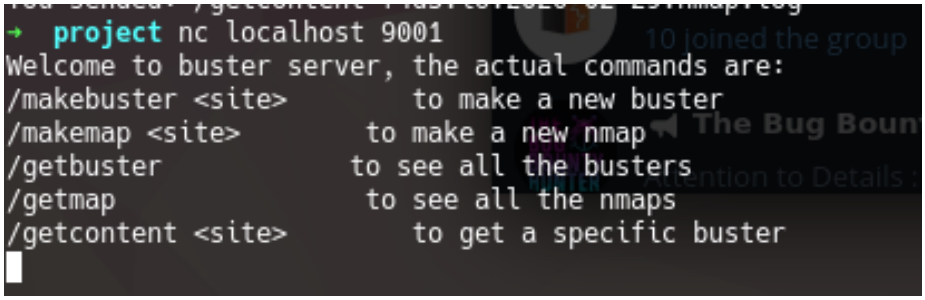
## Introducción

El proyecto se trata de hacer un centro de comandos que permita, administrar escaneos de puertos y mapeos de sitios remotamente, para esto se utilizó lo aprendido en el curso en cuanto a `java` y `websockets`, lo cual permitió llegar a una solución la cual permite, correr y leer outputs de `nmap` y `dirsearch` remotamente.

## Bosquejo de la solución

De manera por defecto, el programa correrá en el puerto `9001`, esto para no necesitar permisos de `root` para lograr correr el programa. De la misma manera, como aún no se ha decidido bajo qué directorio cerrerá el programa, tiene que haber de antemano un directorio en `/tmp/project`, el cual servirá para albergar los outputs del programa. En un futuro esto perfectamente podría cambiar a ser : `$HOME/.remote_buster`.

El programa cuenta con 5 comandos específicos:




- /makebuster
- Comando que permite iniciar un nuevo buster, del modo que se guardará el output respectivo de `dirsearch` con el formato `dominio.fecha.buster.log`
- /makemap
- Comando que permite iniciar un nuevo escaneo de puerto a un sitio arbitrario, el output de `nmap`, quedará guardado del modo formato: `dominio.fecha.nmap.log`
- /getbuster
- comando que permite conseguir todos los busters ya hechos.

- /getmap
- Comando que permite conseguir todos los mapeos ya hechos
- getcontent
- Comando que permite conseguir el output de algún `buster` o `mapeo` ya terminado

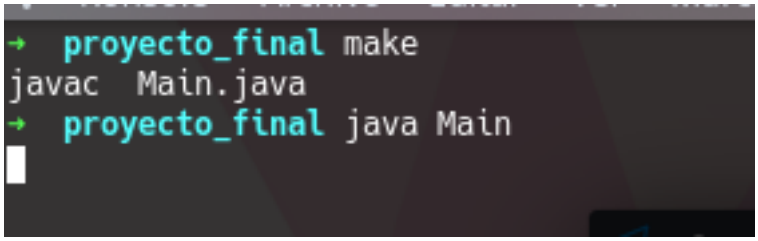
Para conseguir mejor rendimiento del programa, se utilizó paralelismo haciendo que cada nueva conexión entrante sea atendido con un nuevo `hilo`, utilizando `threads`.

# Ejemplo de uso

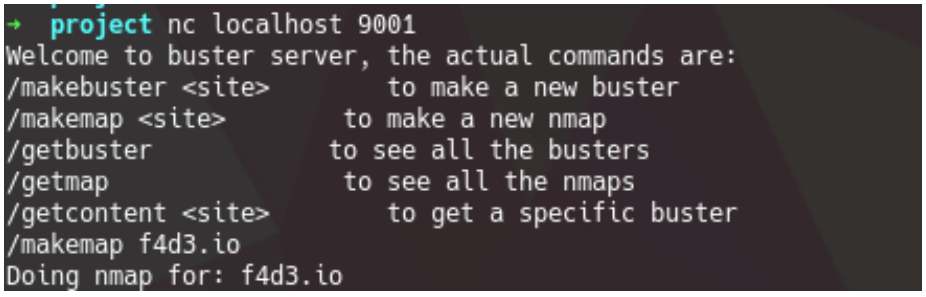
## Para correr el programa

```
make
java Main
```

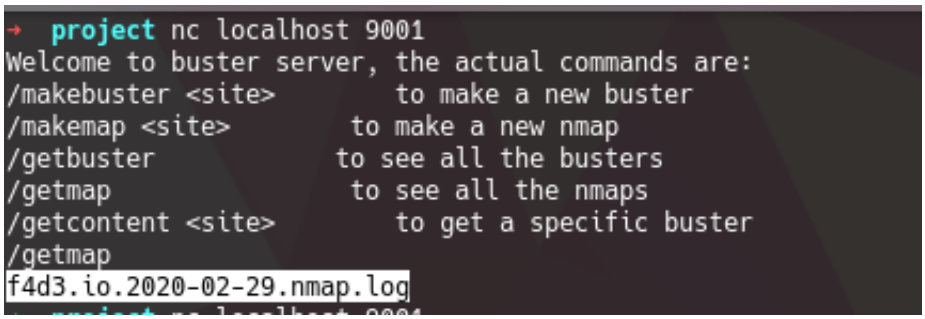
Con esto, dejaremos el servidor corriendo en el puerto `9001`.



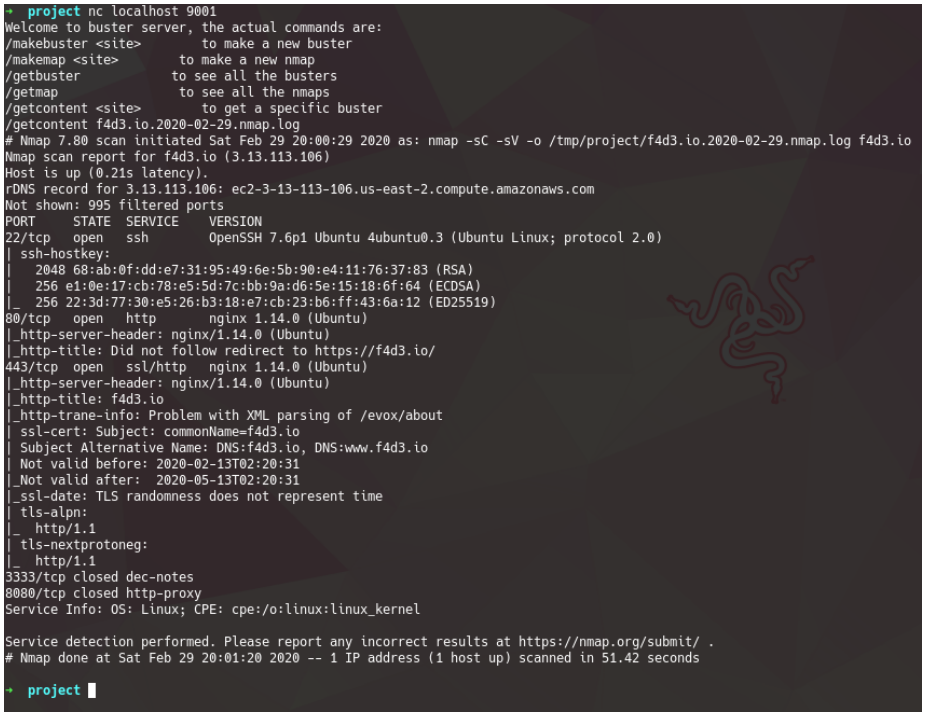

Al conectarnos al servidor, nos dará el banner simple, por lo que correremos un nuevo scan nmap.




Luego podremos consultar por el archivo si este ya terminó.




Como ya terminó, y nos ha devuelto los `.log` de `nmap` almacenados hasta el momento, los podremos ver




Para limpiar todo:

```
make clean
```

## Conclusión

Con esto, podemos administrar de manera fácil y simple la creación de nuevos `busters/mapeos`, como también, iniciar nuevos `on the fly`, sin la necesidad de estar dentro del servidor utilizado para realizarlos.

## TODO things

En un futuro, lo principal a lograr sería poder administrar los actuales `procesos corriendo`, pudiendo pararlos si están consumiendo mucho recurso, con el objetivo de optimizar de buena manera el uso del servidor.