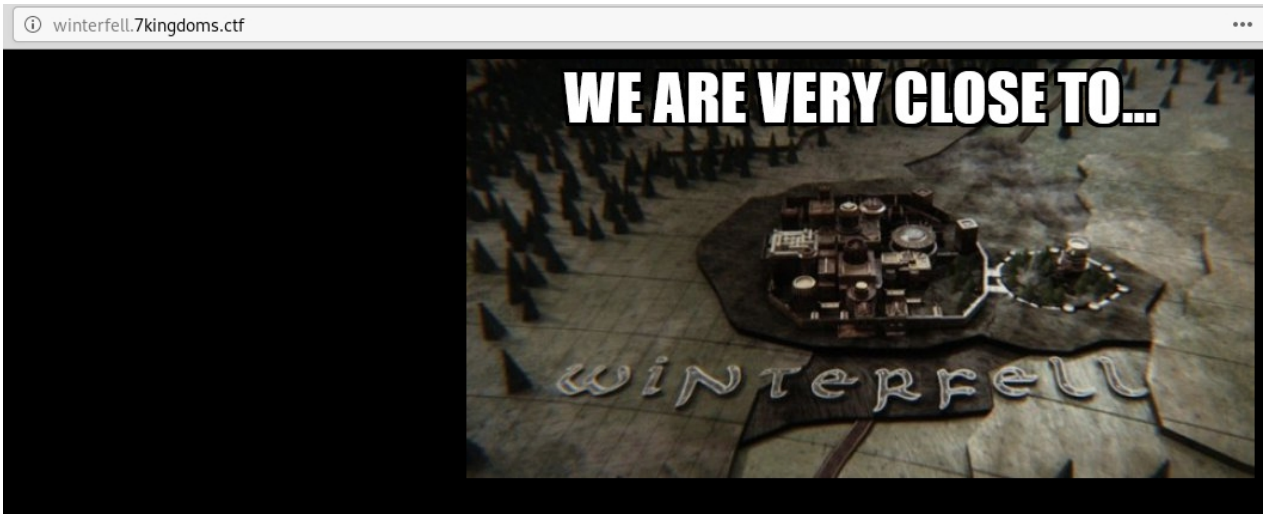
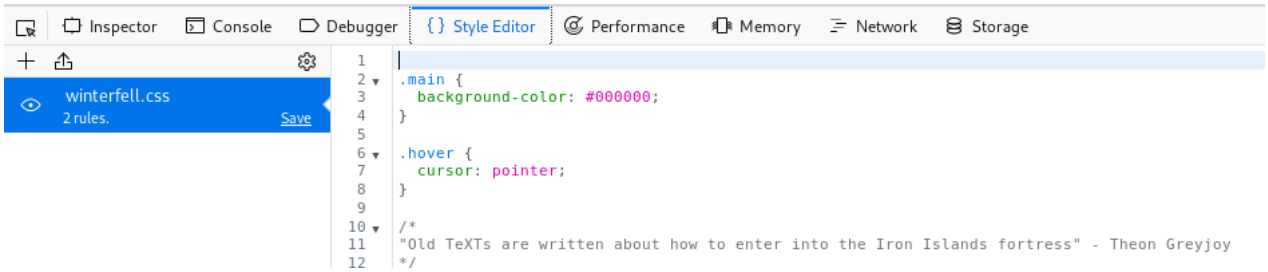
WRITE-UP GOT CTF VULNHUB

ELABORADO POR: ARSENICS

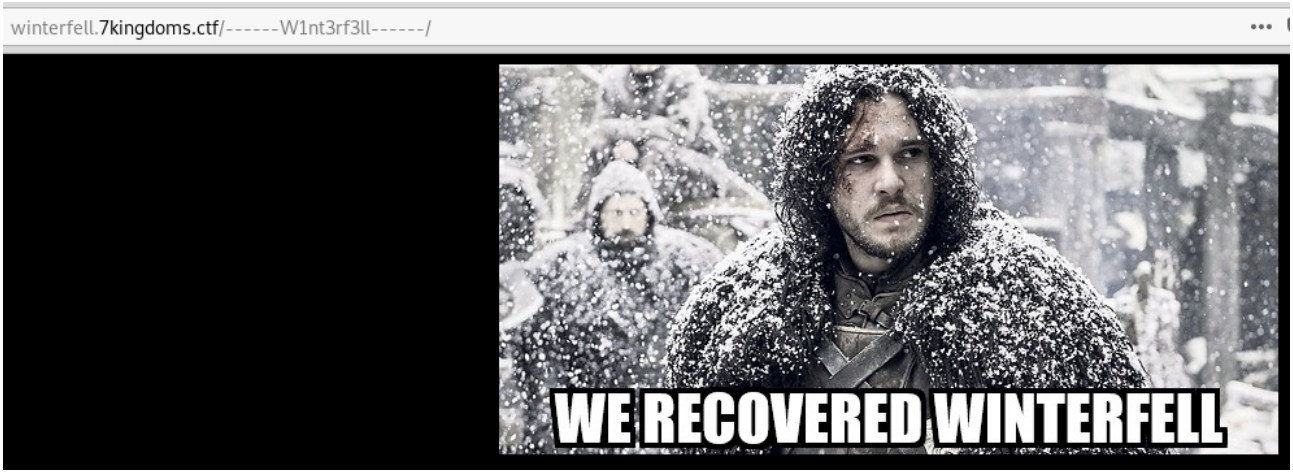
Tercera Fase The Iron Islands : DNS Flag

En la búsqueda de la anterior flag encontramos la primera pista que nos habla de las Iron Islands relacionandolas con los TXT al inspeccionar el elemento como viene siendo la filosfia del rastro de pistas anteriores. Concretamente en el css del style editor:





Del subdominio sacamos la imagen del stark_shield donde con un strings obtenemos la siguiente información:

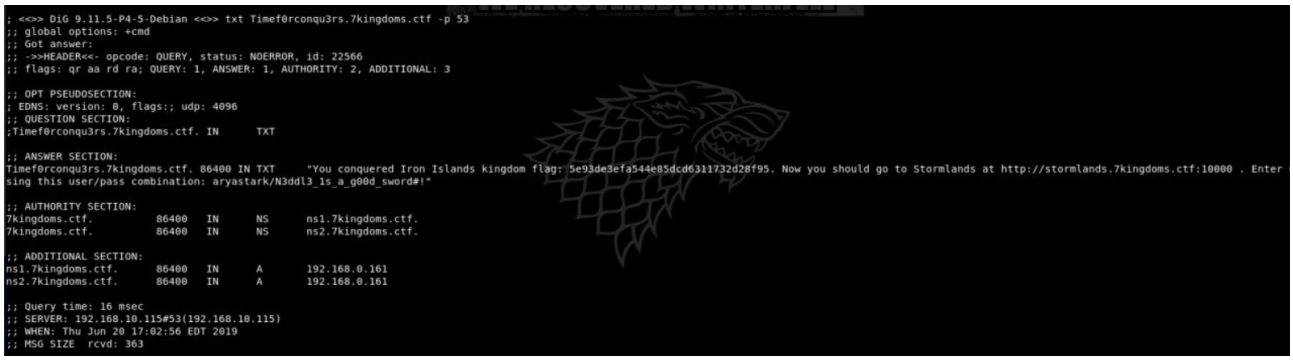


Strings Stark_shield.jpg

```
17:>
qws#K,
drU3
f92jw.O
)99<
"Timef0rconqu3rs TeXT should be asked to enter into the Iron Islands fortress" - Theon Grey
joy
```

Viendo esta nueva pista me percato del camino. Hay que hacer un dig para conseguir ese TXT del dns. Cambiando el resolv.conf con el nameserver a la ip que atacamos y rápidamente tenemos nuestro tesoro la flag de las Iron Islands.

Dig txt Timef0rconqu3rs .7kingdoms.ctf -p 53



De aquí sacamos varias cosas:

a) La flag de Iron Islands.

b) la url de Stormlands en el puerto 10000 (next target) el cuál habíamos visto el webmin en nmap al principio.

c) El user y el pass para el webmin de Stormlands. Let's go!!

```
flag: 5e93de3efa544e85dcd6311732d28f95
```

Autoría: *Arsenics*