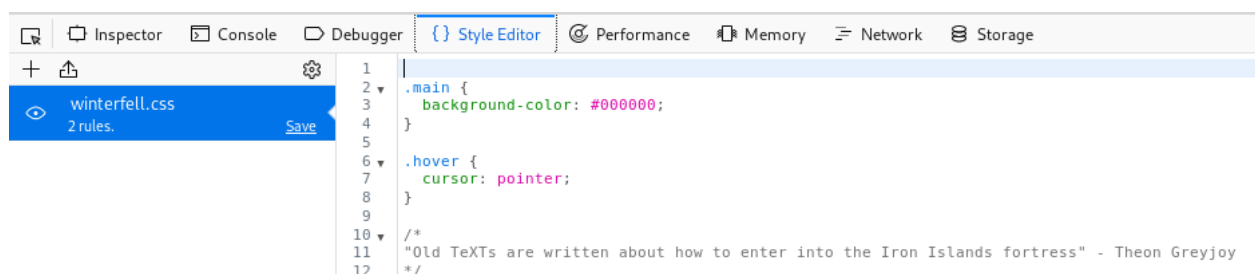
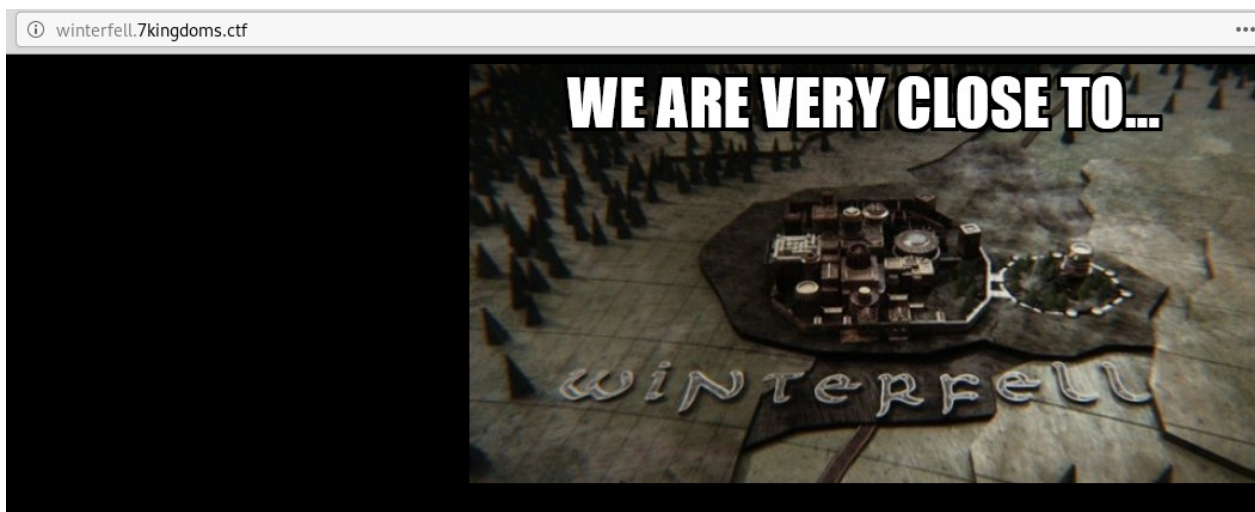


WRITE-UP GOT CTF VULNHUB

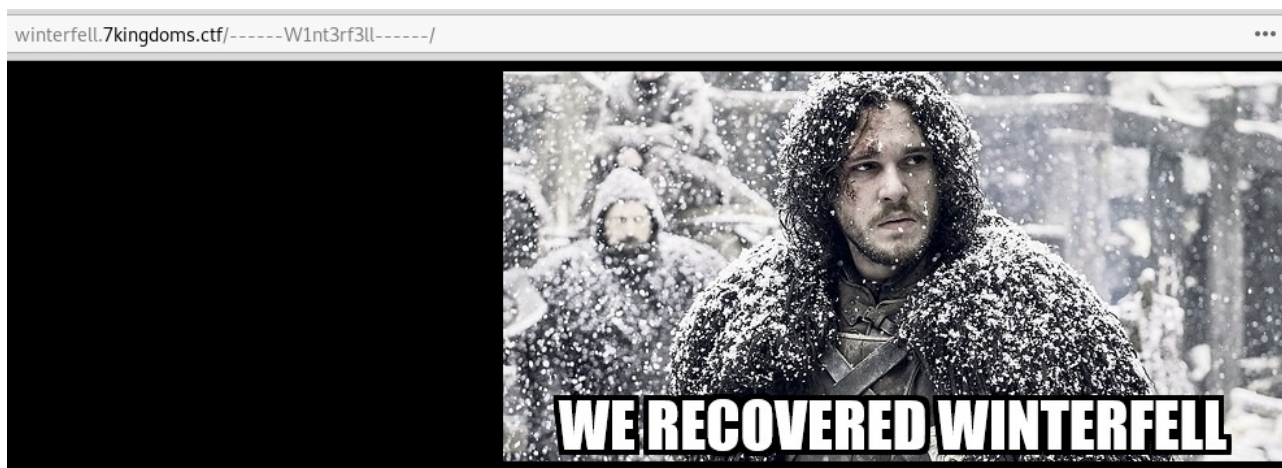
ELABORADO POR: ARSENIC

Tercera Fase The Iron Islands : DN\$ 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 filosofía 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.0
)99<
"Timef0rconqu3rs TeXT should be asked to enter into the Iron Islands fortress" - Theon Grey
joy
```

Viendo esta nueva pista me percató 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

```
;; <<>> Dig 9.11.5-P4-5-Debian <<>> txt Timef0rconqu3rs.7kingdoms.ctf -p 53
;; global options: +cmd
;; got answer:
;; -->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22566
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 4096
;; QUESTION SECTION:
;Timef0rconqu3rs.7kingdoms.ctf. IN      TXT
;; ANSWER SECTION:
Timef0rconqu3rs.7kingdoms.ctf. 86400 IN TXT      "You conquered Iron Islands kingdom flag: 5e93de3efa544e85dcd6311732d28f95. Now you should go to Stormlands at http://stormlands.7kingdoms.ctf:10000 . Enter
sing this user/pass combination: arystark/N3ddl3_is_a_g00d_sword!"
;; AUTHORITY SECTION:
7kingdoms.ctf. 86400 IN NS      ns1.7kingdoms.ctf.
7kingdoms.ctf. 86400 IN NS      ns2.7kingdoms.ctf.
;; ADDITIONAL SECTION:
ns1.7kingdoms.ctf. 86400 IN A      192.168.0.161
ns2.7kingdoms.ctf. 86400 IN A      192.168.0.161
;; Query time: 16 msec
;; SERVER: 192.168.10.115#53(192.168.10.115)
;; WHEN: Thu Jun 20 17:02:56 EDT 2019
;; MSG SIZE rcvd: 363
```

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