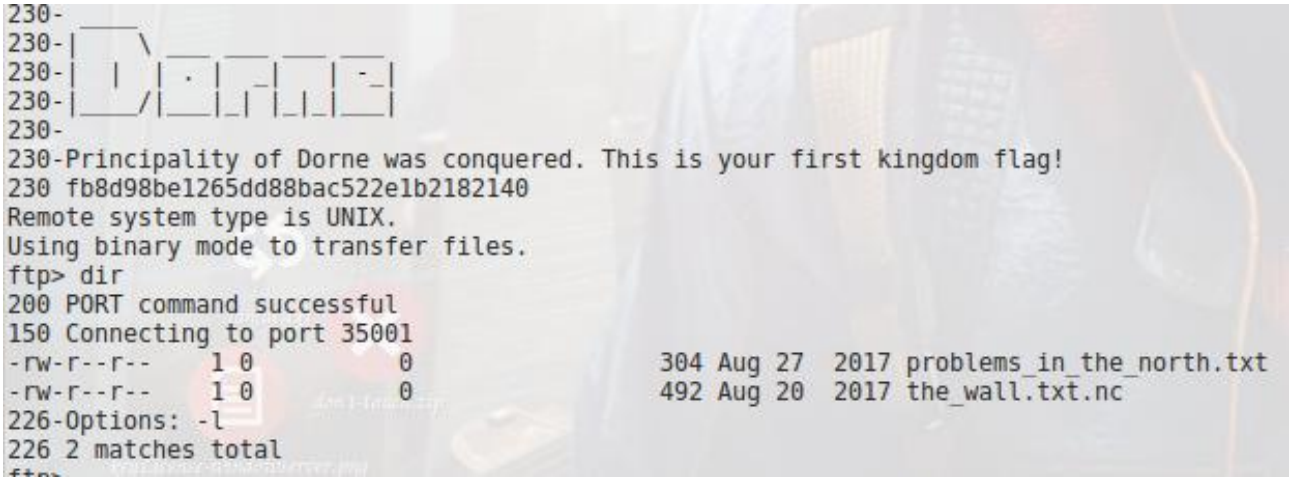
Write ups

CTF VM Game Of Thrones 1.0

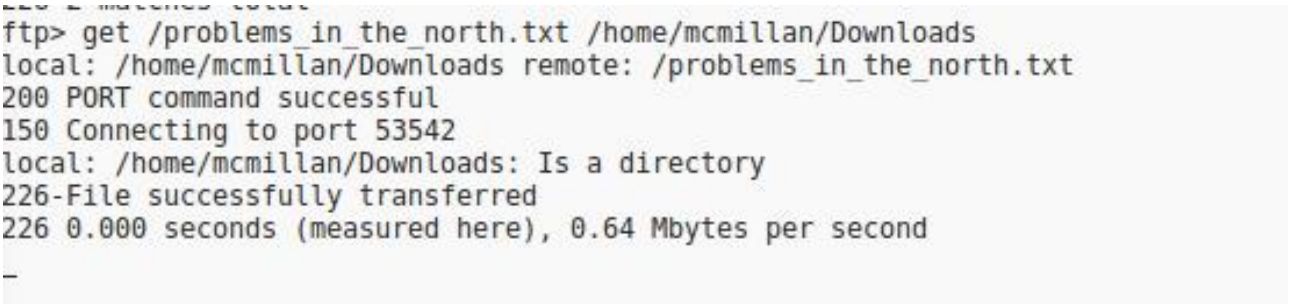
Sulawesi I.T Security** & **iL7Team

Target sudah di set dengan :
Target : 192.168.56.102 - 7kingdoms.ctf
*Machine Target dijalankan di virtualBox dengan set jaringan **Host-only Adapter.***
The wall_the north & iron island

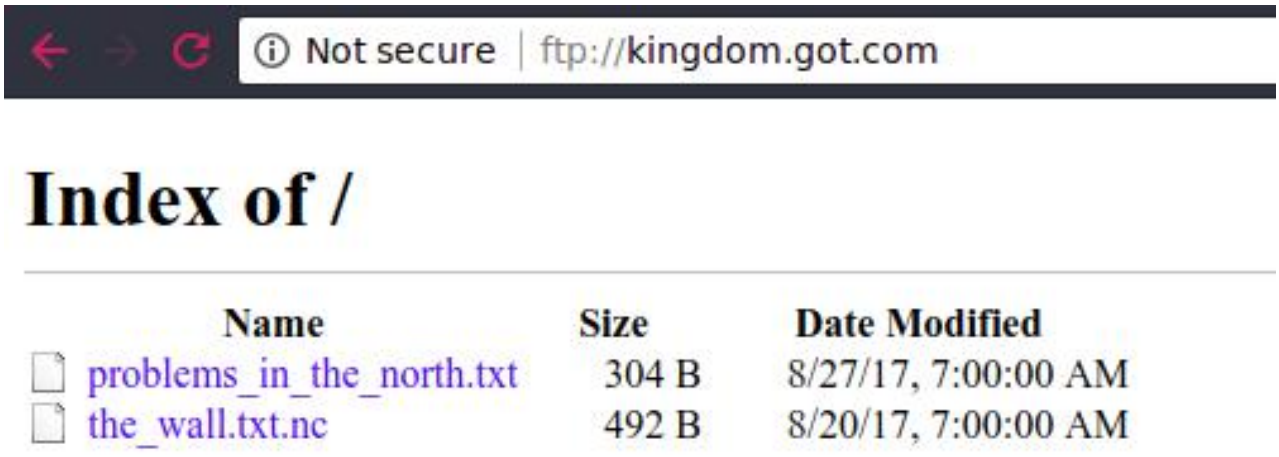


Didalam server ftp nya ada 2 file , txt dan .nc yang terenkripsi.

*Dari sini kita harus menggunakan command ftp, command ini khusus dan hampir sama dengan command linux biasanya. Nah jadi di command ftp ada yang namanya **get** ini perintah untu mengambil file yang ada di server ftp*



Kita juga bisa mengakses ftp nya dari browser kita, ftp://ipaddress atau ftp://kingdom.GOT.com. ingat ya kingdom.GOT.com <- ini sudah saya set dari file ***/etc/hosts***



Sudah saya kasih tau tadi bahwa ada 1 file yang ter encryp , nah jadi kita harus

Untuk menggunakan file .nc kita pakai tools ***mcrypt*** *sesuai dengan arahan petunjuk sebelumnya dan ingat, file yang ter encrypt pastinya meminta password untuk membuka encrypt nya*

```
mcmillan@xeCURIty:~/Downloads/nc$ mcrypt -d the_wall.txt.nc
Enter passphrase:
MD5 check failed
File the_wall.txt.nc was NOT decrypted successfully.
mcmillan@xeCURIty:~/Downloads/nc$ _
```

Jadi kita abaikan saja dulu file yang ter encrypt, . Menariknya kita membuka file .txt nya ada password yang ter encrypt

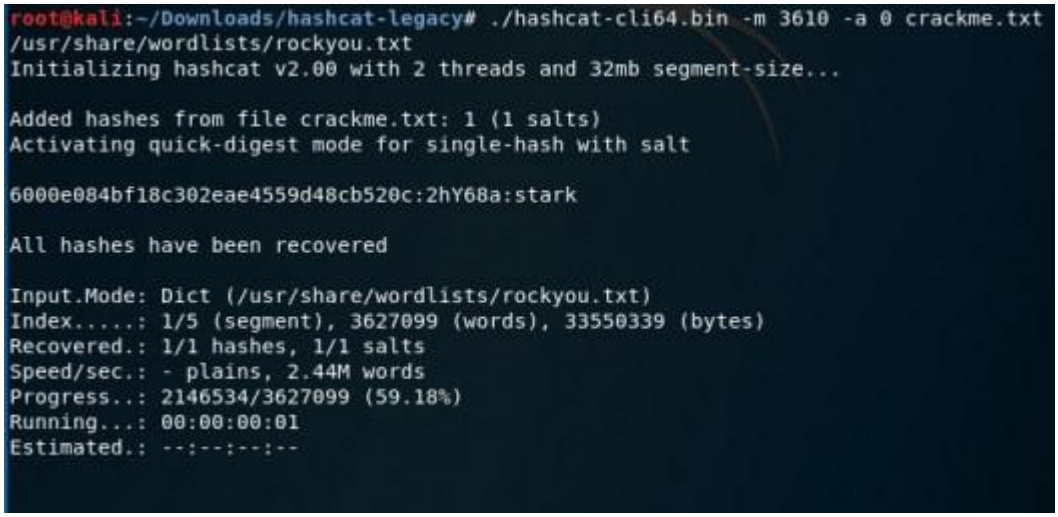
```
"What kind of magic is this?!? I never saw before thi
it carefully" - Maester Aemon Targaryen

md5(md5($s).$p)

nobody:6000e084bf18c302eae4559d48cb520c$2hY68a
```

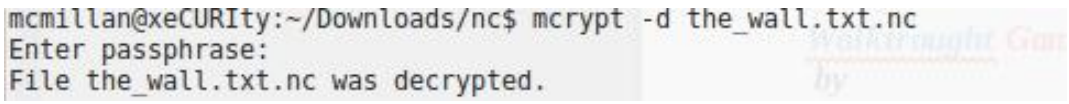
Md5(md5($s).$p) *maksudnya* ***md5(md5($salt).$password)***

Menarik sekali untuk kita cracking, ***Md5(md5($s).$p)*** *kita menggunakan tool* ***hascat*** *atau juga bisa pakai tools favorite kalian, nah ada namanya tool yamg dibuat pake php language dan menjalankannya dari terminal.*

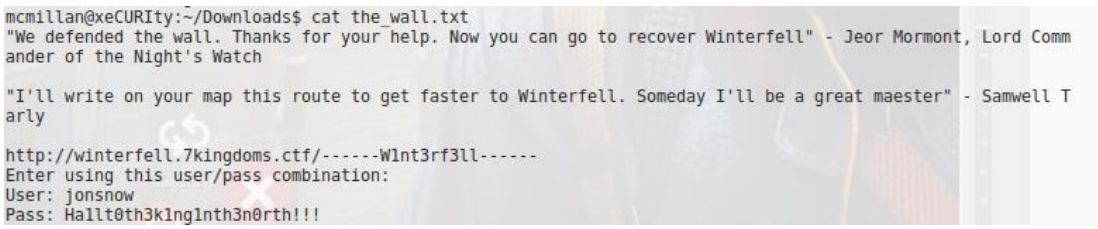


Gambar diatas menunjukan bahwa kita tidak menggunakan tool hashcat bawaan dari kali linux, tapi kita menggunakan ***hashcat-legacy,*** *.*

Tapi kita lihat bahwa kita berhasil meng crack password nya. Dan password nya ini untuk file .nc yang ter encrypt tadi, password : stark



Jika berhasil ter decrypt maka Otomatis langsung keluar keluar .txt



Gawww!!! Thanks raven. http://winterfell.7kingdoms.ctf/------W1nt3rf3ll------ kita ditunjuk langsung untuk pergi ke web tersebut.


```
</body>
</html>
<!--
    "You'll never arrive to Winterfell on that direction. It seems you never learned to read" - The Hound

    "What are you saying? VirtualHost? What the hell is that? Did you get drunk again?" - Gregor (The Mountain) Clegane
-->
```

Dan jika kita bongkar source code nya tidak ada hasil sama sekali.

Damn!! Sampai" bongkar file img nya,, dan tidak dapat petunjuk, dan kita coba lagi crawling dan mengganti wordlist lainnya. Dan it's not work... Why ?

*Jika kita teliti lagi bahwa ada petunjuk di source code nya, "you'll never arrive to winterfell on that direction". "**Arrive to winterfell**". Jika kita tambahkan lagi diujung url **/winterfell** maka notfound.*

*Tapi, kita jangan lupa dengan subdomain, oke kita bermain dengan subomain. Tapi ingat jangan lupa set kembali file yang ada di "**/etc/hosts"** .*

```
192.168.56.102 winterfell.7kingdoms.ctf

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

```
mcmillan@xeCURIty:~/Downloads/nc$ cat the_wall.txt
"We defended the wall. Thanks for your help. Now you can go t
erfell" - Jeor Mormont, Lord Commander of the Night's Watch

"I'll write on your map this route to get faster to Winterfel
l be a great maester" - Samwell Tarly

http://winterfell.7kingdoms.ctf/------W1nt3rf3ll------
Enter using this user/pass combination:
User: jonsnow
Pass: Ha1lt0th3k1ng1nth3n0rth!!!
```

Lihat dia minta memasukan ***http://winterfell.7kingdoms.ctf/------W1nt3rf3ll------***

Saya udah mencoba untuk men set dengan seperti domain sebelum nya, tapi gak bisa juga.


```
8           <link rel="stylesheet" type="text/css" href="../winterfell.css">
9       </head>
10      <body class="main">
11          <center>
12              <img src="meme7.jpg"/>
13          </center>
14          <center>
15              <img src="stark_shield.jpg"/>
16          </center>
17      </body>
18      </html>
19      <!--
20          Welcome to Winterfell
21          You conquered the Kingdom of the North. This is your second kingdom flag!
22          639bae9ac6b3e1a84cebb7b403297b79
23
24          "We must do something here before travelling to Iron Islands, my lady" - Podrick Payne
25
26          "Yeah, I can feel the magic on that shield. Swords are no more use here" - Brienne Tarth
27      -->
```

Kita mendapatkan flag kingdom kedua : 639bae9ac6b3e1a84cebb7b403297b79

Upss.. Tapi mari kita lihat apa yang dia bilang,,, "sebelum ke pulau iron, kita harus lakukan sesuatu disini" "i can feel magic on that shield". Intinya kita harus bongkar .jpg yang gambar harimau itu.

```
f92jw.O
)99<
"Timef0rconqu3rs TeXT should be asked to enter into the Iron Islands fortress" -
 Theon Greyjoy
mcmillan@xeCURIty:~/Downloads/game-of-thrones$ strings shield.jpeg _
```

Timef0rconqu3rs TeXT harus diminta untuk masuk ke benteng iron island.

Maksudnya apa ya,, mulai mencari tahu dengan menambahkan diujung url -> Timef0rconqu3rs dan menggantikan sebagai subdomain , tapi gk dapat petunjuk. Tujuan kita sekarang untuk masuk ke iron island yang dimana kita masuk melalui dns. Nah kalau dipikir" kita harus scan dns nya dulu menggunakan tool yang bisa scan dns.

```
mcmillan@xeCURIty:~/Downloads/game-of-thrones$ dig Timef0rconqu3rs.7kingdoms.ctf

; <<>> DiG 9.9.5-3ubuntu0.17-Ubuntu <<>> Timef0rconqu3rs.7kingdoms.ctf
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57523
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;Timef0rconqu3rs.7kingdoms.ctf. IN      A

;; AUTHORITY SECTION:
7kingdoms.ctf.          86400   IN      SOA     ns1.7kingdoms.ctf. ns2.7kingdoms.ctf. 2017072301
21600 3600 604800 86400

;; Query time: 0 msec
;; SERVER: 192.168.56.102#53(192.168.56.102)
;; WHEN: Sat May 19 23:06:32 WIB 2018
;; MSG SIZE  rcvd: 102
```

Sama sekali tidak dapat petunjuk, tapi kita harus teliti lagi dengan yang diminta oleh ***Thon Greyjoy,*** *Timef0rconqu3rs TeXT , nah dalam dns ada namanya record/rekaman... Di dns ada namnya rekaman A , IN, NS, SOA & TXT*

```
mcmillan@xeCURIty:~/Downloads/game-of-thrones$ dig Timef0rconqu3rs.7kingdoms.ctf txt

; <<>> DiG 9.9.5-3ubuntu0.17-Ubuntu <<>> Timef0rconqu3rs.7kingdoms.ctf txt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65146
;; 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: 5e93de3
efa544e85dcd6311732d28f95. Now you should go to Stormlands at http://stormlands.7kingdoms.ctf:100
00 . Enter using this user/pass combination: aryastark/N3ddl3_1s_a_g00d_sword#!"

;; AUTHORITY SECTION:
7kingdoms.ctf.          86400   IN      NS      ns2.7kingdoms.ctf.
7kingdoms.ctf.          86400   IN      NS      ns1.7kingdoms.ctf.

;; ADDITIONAL SECTION:
ns1.7kingdoms.ctf.      86400   IN      A       192.168.56.102
ns2.7kingdoms.ctf.      86400   IN      A       192.168.56.102

;; Query time: 0 msec
;; SERVER: 192.168.56.102#53(192.168.56.102)
;; WHEN: Sat May 19 23:07:32 WIB 2018
;; MSG SIZE  rcvd: 363
```

"You conquered Iron Islands kingdom flag: 5e93de3efa544e85dcd6311732d28f95. Now you should go to Stormlands at http://stormlands.7kingdoms.ctf:10000 . Enter using this user/pass combination: aryastark/N3ddl3_1s_a_g00d_sword#!"

Iron Islands kingdom flag: ***5e93de3efa544e85dcd6311732d28f95***