WRITE-UP GOT CTF VULNHUB

ELABORADO POR: ARSENICS

Segunda Fase The Wall & The North: HTTP flag

Dentro del FTP al hacer dir nos aparecen 2 txt interesantes. Los descargo con wget:

```
230-OK. Current directory is /
230-Welcome to:
230-  ____
230-|    \ ___ ___ ___ ___
230-|  |  | . |  _|   | -_|
230-|____/|___|_| |_|_|___|
230-
230-Principality of Dorne was conquered. This is your first kingdom flag!
230 fb8d98be1265dd88bac522e1b2182140
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful
150 Connecting to port 41699
-rw-r--r--    1 0          0               304 Aug 27  2017 problems_in_the_north.txt
-rw-r--r--    1 0          0               492 Aug 20  2017 the_wall.txt.nc
226-Options: -l
226 2 matches total
```

Cat problems_in_the_north.txt

```
"There are problems in the north. We must travel quickly. Once there we must defend the wall" - Jon Snow

"What kind of magic is this?!? I never saw before this kind of papirus. Let's check it carefully" - Maester Aemon Targaryen

md5(md5($s).$p)

nobody:6000e084bf18c302eae4559d48cb520c$2hY68a
```

De aquí se obtiene la pass para descifrar el mcript que tenemos el the_wall.txt. Es un md5 que envuelve otro md5 con formato de salto y password. Si se investiga un poco se halla que el modelo 3610 de hashcat es justo este formato. La versión original de hashcat no soporta el 3610 pero hay otra versión hashcat legacy que lo integra.

Hashcat -m 3610 -a 0 gothash.txt /usr/share/wordlists/rockyou.txt

6000e084bf18c302eae4559d48cb520c:2hY68a:stark

Cat the_wall.txt

```
m@rijndael-128 cbcmcrypt-sha1B0_0900WB0[nF09040md5#N-0}
                                                  06061f00>0oh0000y<Z80000\0000N00000Ab00
              Tq2a0l000100 700}Fjs0I0@ 0rLS0tgh7M0CSu0|9c00n0-0I
0nv0\Q0I0000Pcf000000*ag{00kT0(y00w00000        u000Dd>y0@'0#И$00
                                                  000000000lw0Y$0<00A)0^$00:6DV2       0s;000sW00000o00U01Wo0x{=)10Tp03000((08ɔs0H00y&0003Ø")db3G
g00/00&*U00}G000:0: 0040900榕 0
                 00r
                    000000000

                          !008#000(|0k\    00<0Vpf 0w
```

Luego por lo que se puede leer es un mcrypt como habíamos visto en una de las pistas cuando estabamos recogiendo información en la web del puerto 80 y concretamente vemos que es un Rijndael 128- CBC. Se prueba una tool online que no ofrece el resultado esperando y se termina realizando un script en php para hallar el resultado.

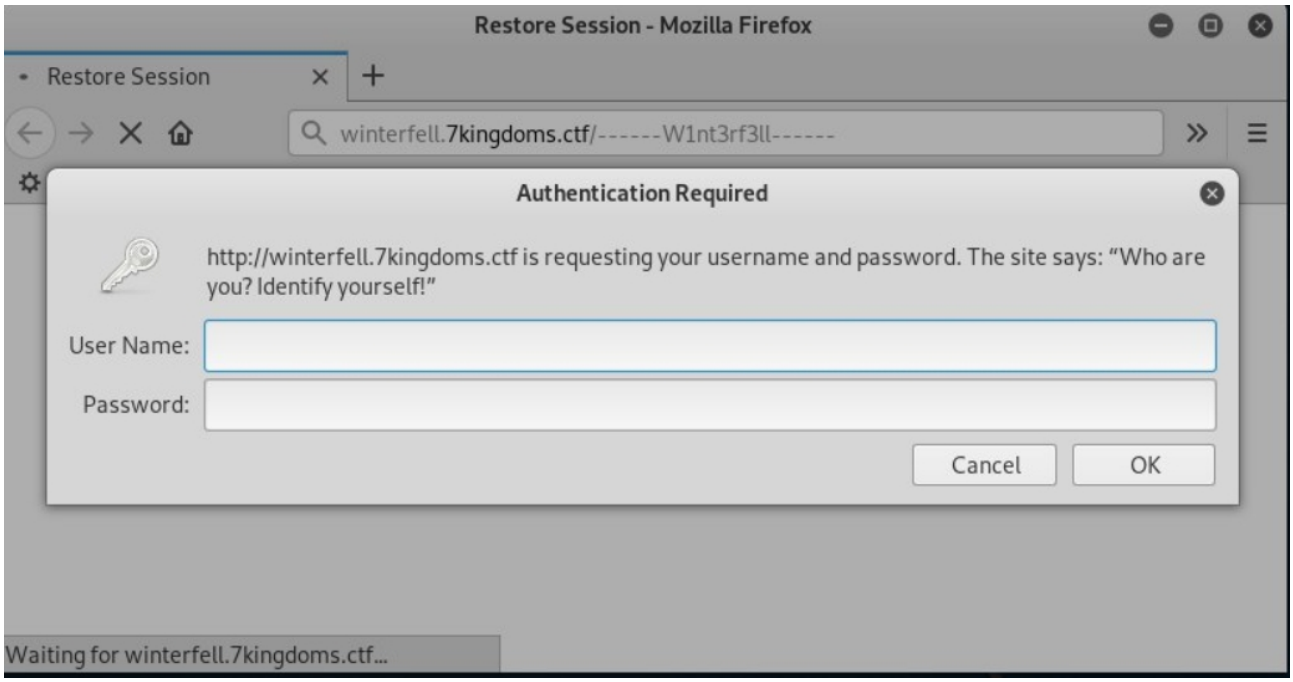
```
root@kali:~/ftp_got# cat the_wall.txt
"We defended the wall. Thanks for your help. Now you can go to recover Winterfell"
 - Jeor Mormont, Lord Commander of the Night's Watch

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

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

Vaya, vaya, habemus link, user y pass alltogether para no marear al personal, perfecto, no??

Directamente no resuelve la web, pero si la introducimos en el etc/hosts se solventa el problema.



Entramos con el user y pass de jonsnow. Voilà ya tenemos la segunda flag!!

```
<!DOCTYPE HTML>
    <html>
    <head>
        <title>Game of Thrones CTF</title>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
        <link rel="shortcut icon" href="favicon.ico">
        <link rel="stylesheet" type="text/css" href="../winterfell.css">
    </head>
    <body class="main">
        <center>
            <img src="meme7.jpg"/>
        </center>
        <center>
            <img src="stark_shield.jpg"/>
        </center>
    </body>
    </html>
    <!--
        Welcome to Winterfell
        You conquered the Kingdom of the North. This is your second kingdom flag!
        639bae9ac6b3e1a84cebb7b403297b79

        "We must do something here before travelling to Iron Islands, my lady" - Podrick Payne

        "Yeah, I can feel the magic on that shield. Swords are no more use here" - Brienne Tarth
    -->
```

Magia realizada y segunda flag obtenida. A por la tercera de Iron Islands / dns Flag!!

Autoría: *Arsenics*