GameOfThrones Vulnhub's vulnerable lab challenge

Information Security Inc.

Contents

- About Vulnhub
- Target VM
- Test Setup
- Walkthrough
- References

About Vulnhub

- To provide materials that allows anyone to gain practical 'hands-on' experience in digital security, computer software & network administration

Target VM

- Target VM: GameOfThrones
- Download the ova file

https://mega.nz/#!EcgHBB4b!UvbxukV_Po0BOALwqyzxqdpxSfPkIzuxiNqEEVgDy8Q
https://www.vulnhub.com/entry/game-of-thrones-ctf-1,201/

- Import the ova file into your favorite hypervisor;

- Attach a DHCP enabled interface to the machine and run it
- Objective
  Find the flags

Test Setup

◎ Testing environment

Linux Kali (attacker) >>> GameOfThrones (target vm)

Walkthrough

- From the attacker machine run the following command to find out Target VMs IP address:

```
root@LUCKY64:~# netdiscover -i eth0 -r 192.168.44.0
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 6 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 360
 ___________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 ---------------------------------------------------------------------------
 192.168.44.1    00:50:56:c0:00:01      3     180  VMware, Inc.
 192.168.44.133  00:0c:29:f2:a3:46      2     120  VMware, Inc.
 192.168.44.254  00:50:56:ff:49:a0      1      60  VMware, Inc.
```

- Scan the target machine IP (192.168.44.133)

```
root@LUCKY64:~# ./Scan.py
TCP port 21 is open
TCP port 22 is open
TCP port 53 is open
TCP port 80 is open
TCP port 1337 is open
TCP port 5432 is open
TCP port 10000 is open
```

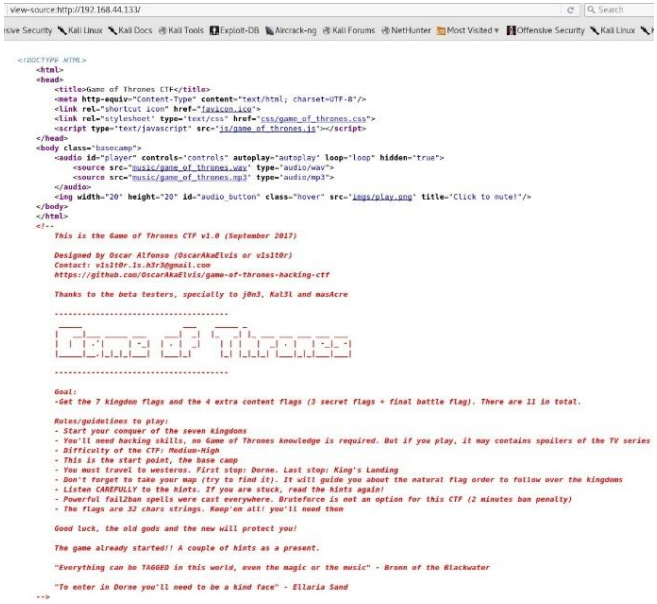
Walkthrough

- Explore Port 80 in a browser

”

Walkthrough

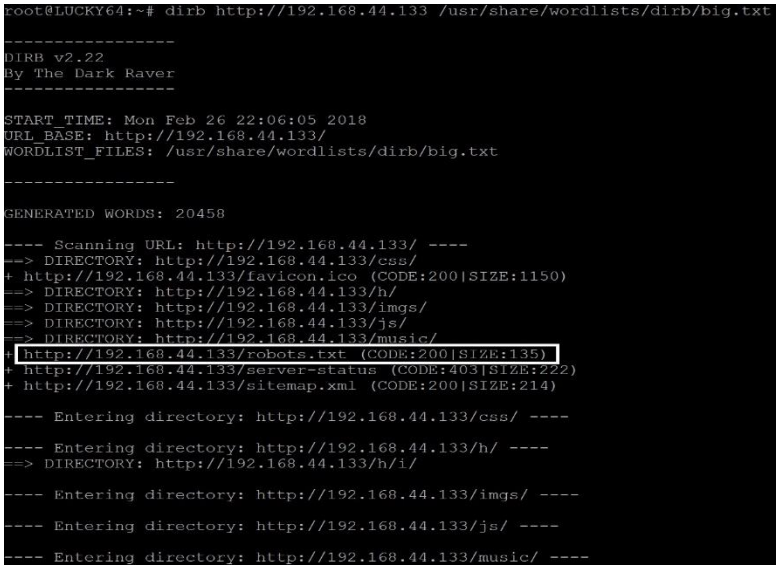
- Explore page source; some hints and brute force is not an option


view-source:http://192.168.44.133/
Search
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Most Visited
Offensive Security
Kali Linux
<!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="css/game_of_thrones.css">
<script type="text/javascript" src="js/game_of_thrones.js"></script>
</head>
<body class="basecamp">
<audio id="player" controls="controls" autoplay="autoplay" loop="loop" hidden="true">
<source src="music/game_of_thrones.wav" type="audio/wav">
<source src="music/game_of_thrones.mp3" type="audio/mp3">
</audio>

</body>
</html>
<!--
This is the Game of Thrones CTF v1.0 (September 2017)
Designed by Oscar Alfonso (OscarAkaElvis or v1s1t0r)
Contact: v1s1t0r.1s.h3r3@gmail.com
https://github.com/OscarAkaElvis/game-of-thrones-hacking-ctf
Thanks to the beta testers, specially to j0n3, Kal31 and masAcre
Goal:
-Get the 7 kingdom flags and the 4 extra content flags (3 secret flags + final battle flag). There are 11 in total.
Rules/guidelines to play:
- Start your conquer of the seven kingdoms
- You'll need hacking skills, as Game of Thrones knowledge is required. But if you play, it may contains spoilers of the TV series
- Difficulty of the CTF: Medium-High
- This is the start point, the base camp
- You must travel to westeros. First stop: Dorne. Last stop: King's Landing
- Don't forget to take your map (try to find it). It will guide you about the natural flag order to follow over the kingdoms
- Listen CAREFULLY to the hints. If you are stuck, read the hints again!
- Powerful fail2ban spells were cast everywhere. Bruteforce is not an option for this CTF (2 minutes ban penalty)
- The flags are 32 chars strings. Keep'em all! you'll need them
Good luck, the old gods and the new will protect you!
The game already started!! A couple of hints as a present.
"Everything can be TAGGED in this world, even the magic or the music" - Bronn of the Blackwater
"To enter in Dorne you'll need to be a kind face" - Ellaria Sand
-->"

Walkthrough

- Use dirb tool to scan the host on port 80; found robots.txt

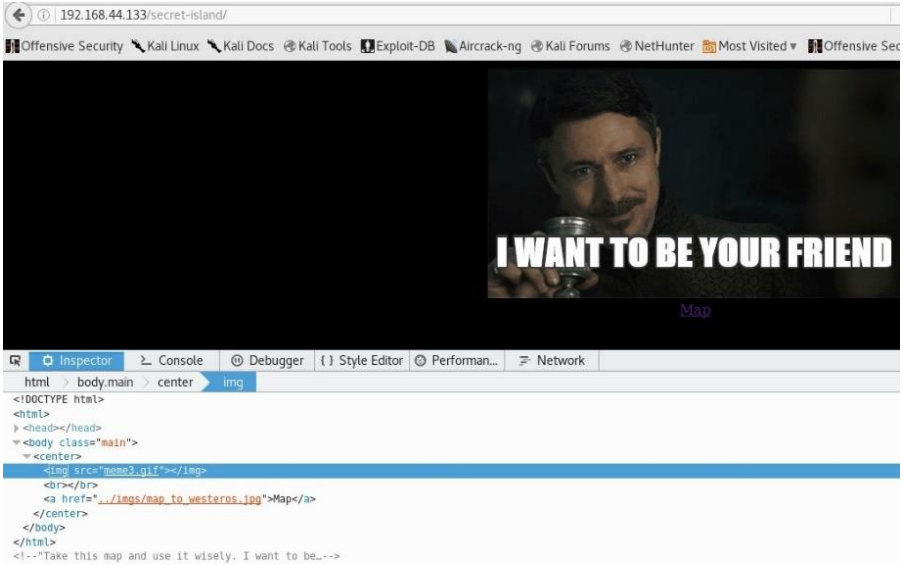


Walkthrough

- Checking robots.txt

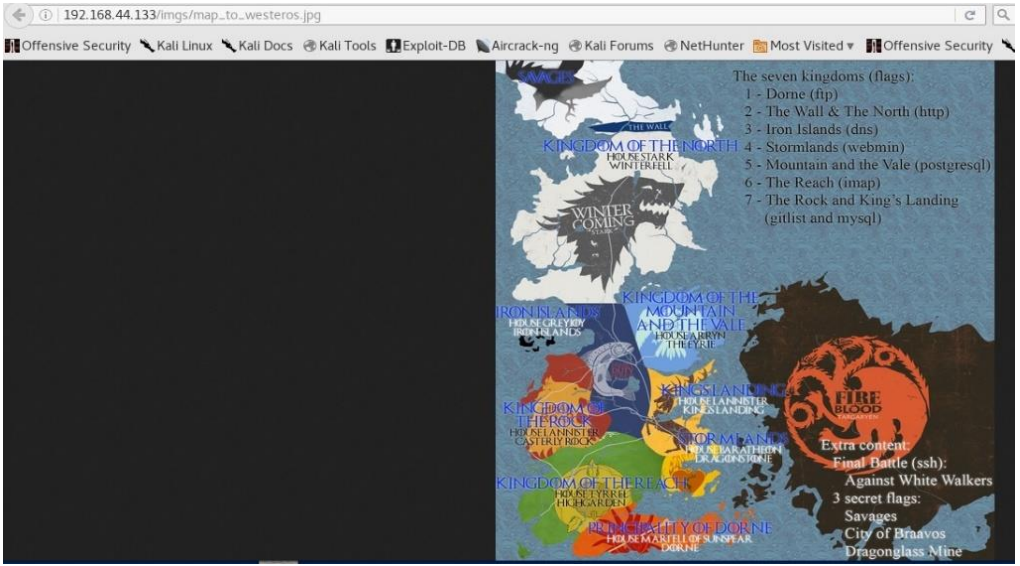
Walkthrough

- Accessing disallowed links => “secret-island” and take the map



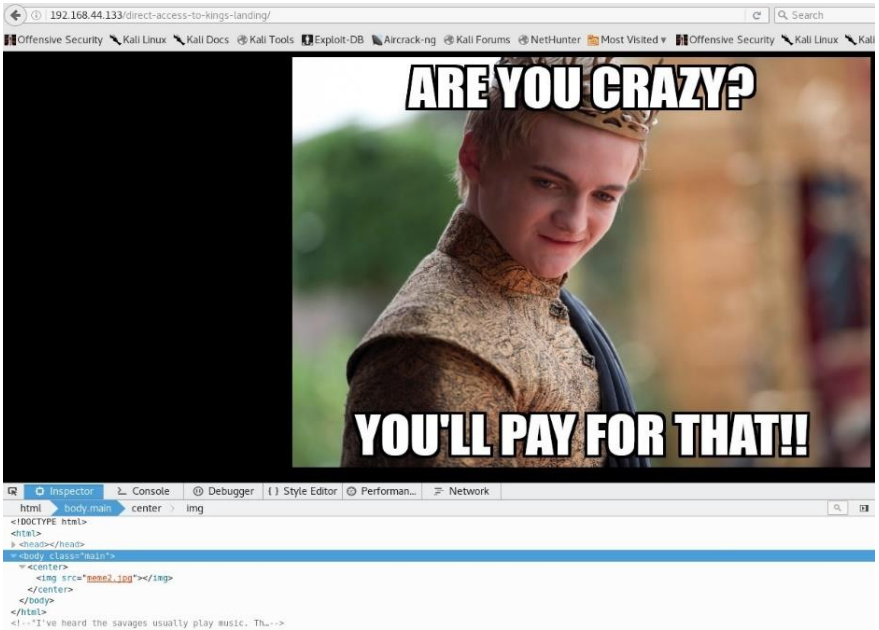
Walkthrough

- Accessing disallowed links => “secret-island” and take the map



Walkthrough

◎ Accessing disallowed links => “direct-access-to-kings-landing”

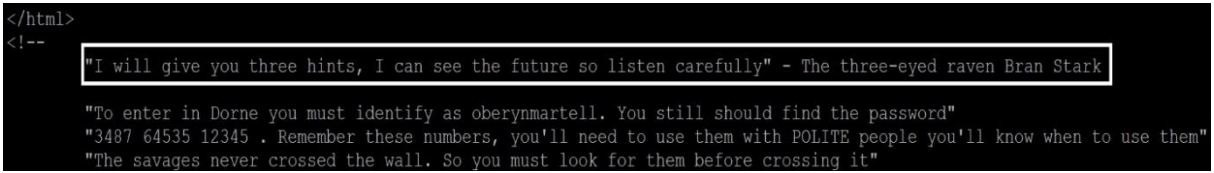


Walkthrough

- Accessing allowed link => “the-tree” , Got a hint which says that we need a different UserAgent when accesing the server

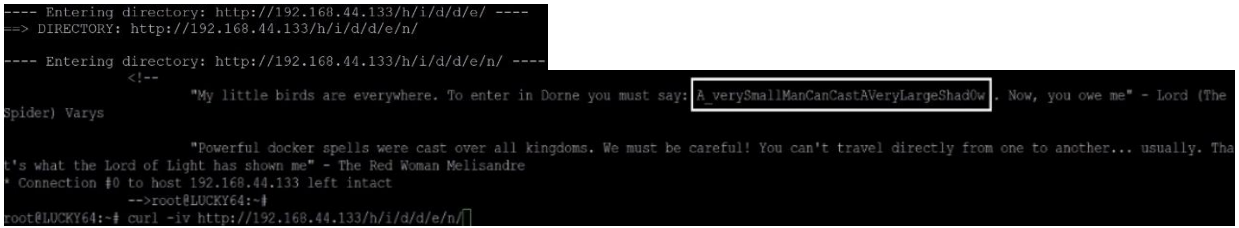
Walkthrough

- Accessing allowed link => “the-tree” using “Three-eyed-raven” UserAgent, got three hints (username and three ports for port knocking https://en.wikipedia.org/wiki/Port_knocking)



Walkthrough

◎ Accessing the “/h/i/d/d/e/n/” directory found by dirb and get the password for oberynmartell: A_verySmallManCanCastAVeryLargeShad0w



Walkthrough

- Use ftp to connect using the acquired username and password and get the first flag

```
root@LUCKY64:~# ftp -n 192.168.44.133
Connected to 192.168.44.133.
220-------------------------
220-"These are the Dorne city walls. We must enter!" - Grey Worm
220-
220-"A fail2ban spell is protecting these walls. You'll never get in" - One of the Sand Snake Girls
220-------------------------
220 This is a private system - No anonymous login
ftp> user
(username) oberynmartell
331 User oberynmartell OK. Password required
Password:
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 33227
-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
```

Walkthrough

- Use ftp to download the files

```
ftp> get problems_in_the_north.txt
local: problems_in_the_north.txt remote: problems_in_the_north.txt
200 PORT command successful
150 Connecting to port 46241
226-File successfully transferred
226 0.024 seconds (measured here), 12.58 Kbytes per second
304 bytes received in 0.02 secs (12.4895 kB/s)
ftp> get the_wall.txt.nc
local: the_wall.txt.nc remote: the_wall.txt.nc
200 PORT command successful
150 Connecting to port 37249
226-File successfully transferred
226 0.021 seconds (measured here), 23.29 Kbytes per second
492 bytes received in 0.02 secs (23.1362 kB/s)
ftp> quit
221-Goodbye. You uploaded 0 and downloaded 1 kbytes.
221 Logout.
```

Walkthrough

- Save the has from one of the downloaded files ()

```
root@LUCKY64:~# 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
root@LUCKY64:~# echo "6000e084bf18c302eae4559d48cb520c$2hY68a" > HashFromFtp
root@LUCKY64:~# cat HashFromFtp
6000e084bf18c302eae4559d48cb520chY68a
root@LUCKY64:~# cat HashFromFtp
6000e084bf18c302eae4559d48cb520c$2hY68a
```

Walkthrough

- Use hashcat to find out the password (stark)

```
root@LUCKY64:~# john --format=dynamic_2008 HashFromFtp
Using default input encoding: UTF-8
Loaded 1 password hash (dynamic_2008 [md5(md5($s).$p) (PW > 23 bytes) 128/128 AVX 4x3])
Press 'q' or Ctrl-C to abort, almost any other key for status
stark            (?)
1g 0:00:00:00 DONE 3/3 (2018-02-27 01:14) 2.380g/s 392930p/s 392930c/s 392930C/s 142400..murum
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

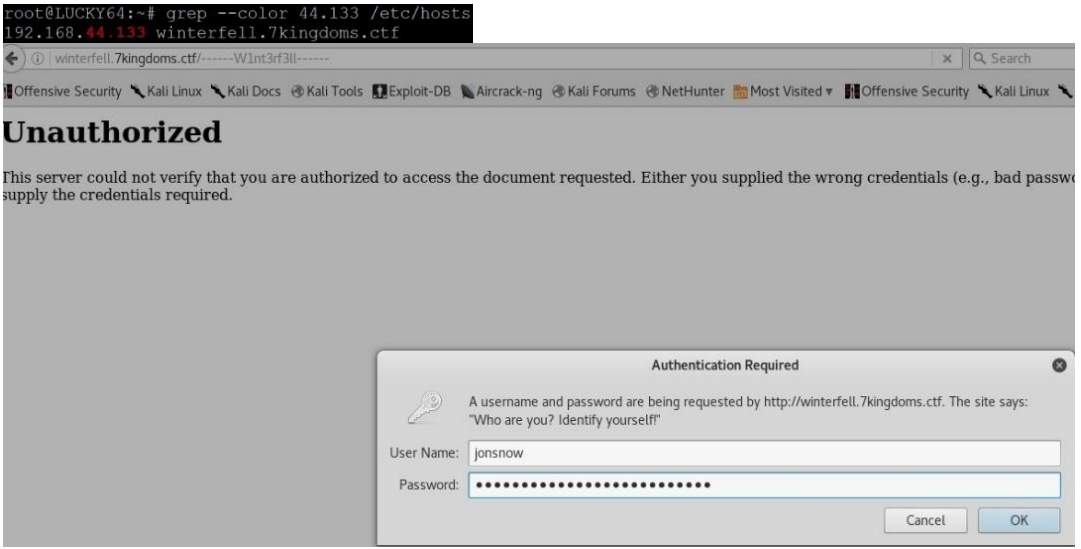
Walkthrough

- Use the password to decrypt the second file downloaded from ftp

```
root@LUCKY64:~# file the_wall.txt.nc
the_wall.txt.nc: mcrypt 2.5 encrypted data, algorithm: rijndael-128, keysize: 32 bytes, mode: cbc,
root@LUCKY64:~# mcrypt -d the_wall.txt.nc
Enter passphrase:
File the_wall.txt.nc was decrypted.
root@LUCKY64:~# 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!!!
```

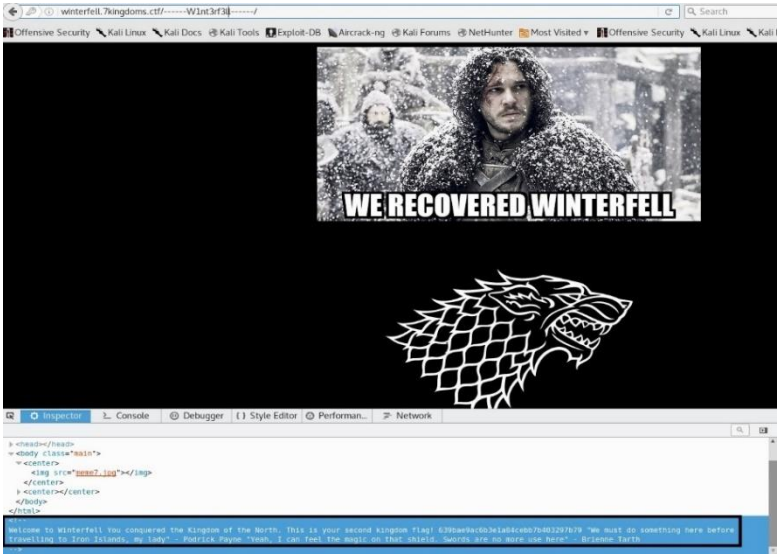
Walkthrough

- Access http://winterfell.7kingdoms.ctf/------W1nt3rf3ll------ and get the second flag



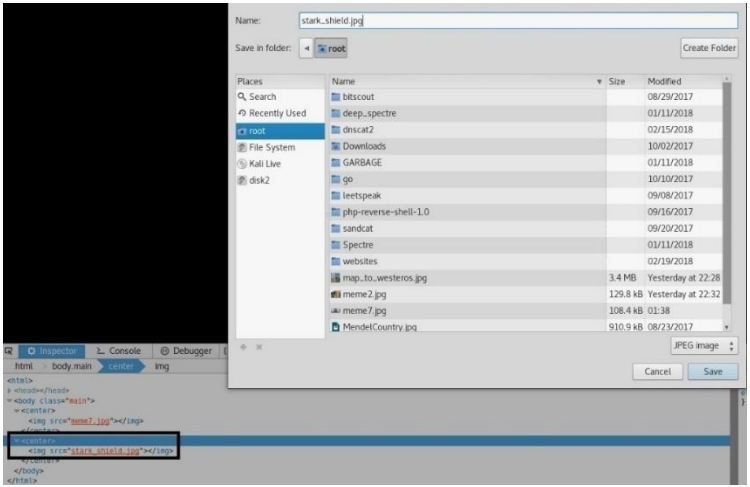
Walkthrough

- Access http://winterfell.7kingdoms.ctf/------W1nt3rf3ll------ and get the second flag



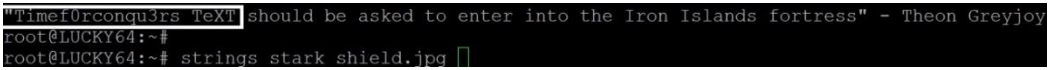
Walkthrough

◎ Download “stark_shield.jpg” and check it using => strings



Walkthrough

◎ Found a domain name => Timef0rconqu3rs



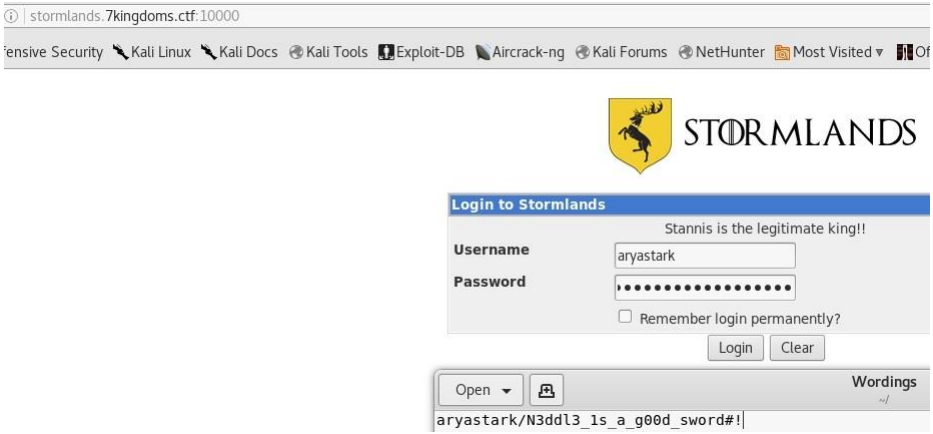
Walkthrough

- Use dig and ask for “Timef0rconqu3rs.7kingdoms.ctf” and get the third flag and obtained another usermame and password

```
root@LUCKY64:~# dig Timef0rconqu3rs.7kingdoms.ctf  @192.168.44.133 TXT

; <<>> DiG 9.10.3-P4-Debian <<>> Timef0rconqu3rs.7kingdoms.ctf @192.168.44.133 TXT
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34000
;; 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 using this user/pass combination: aryastark/N3dd13_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       192.168.44.133
ns2.7kingdoms.ctf.      86400   IN      A       192.168.44.133

;; Query time: 0 msec
;; SERVER: 192.168.44.133#53(192.168.44.133)
;; WHEN: Tue Feb 27 01:48:05 EST 2018
;; MSG SIZE  rcvd: 363
```

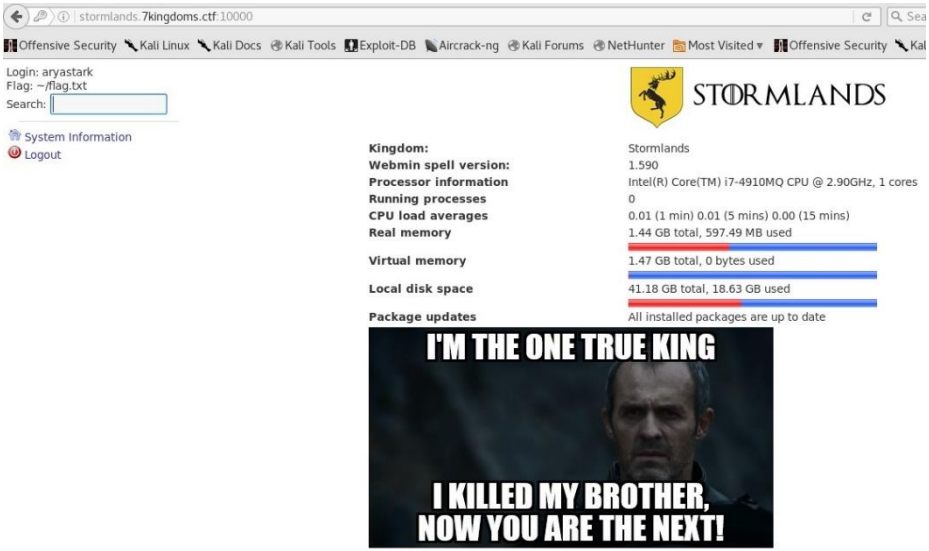
Walkthrough

- Login to stormlands.7kingdoms.ctf:10000



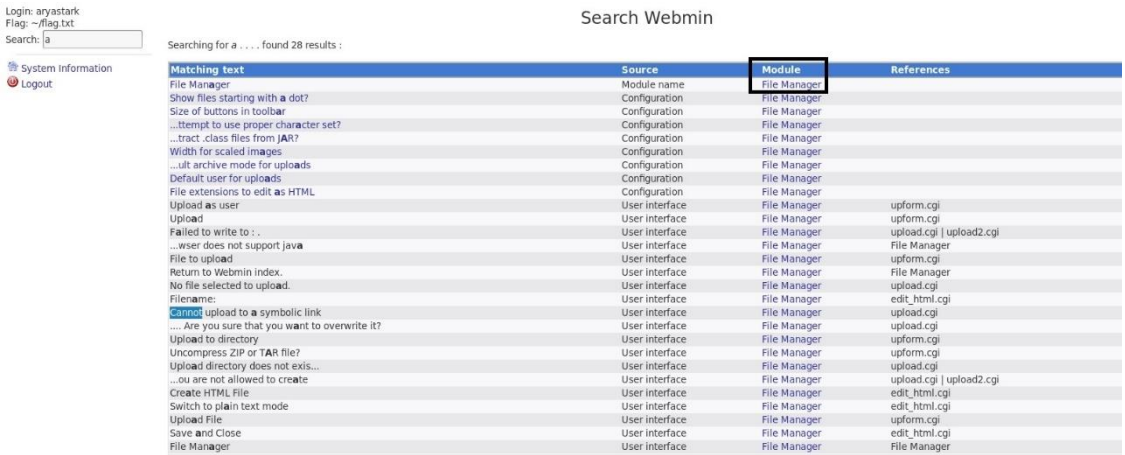
Walkthrough

- Login to stormlands.7kingdoms.ctf:10000



Walkthrough

- Use “search” and look for interesting things, found a FileManager feature



Walkthrough

◎Get another flag from /home/aryastark/flag.txt


Ve download the file and open it in our system and find our 4th flag.

Welcome to:

Congratulations! you conquered Stormlands. This is your flag: 8fc42c6ddf9966db3b09e84365034357

Now prepare yourself for the next challenge!

The credentials to access to the Mountain and the Vale kingdom are:
user/pass: robinarryn/cr0wn_f0r_a_King-_
db: mountainandthevale

pgAdmin magic will not work. Command line should be used on that kingdom - Talisa Maegyr

References

- Vulnhub website
https://www.vulnhub.com

- Vulnerable VM URL
https://www.vulnhub.com/entry/game-of-thrones-ctf-1,201/

- John the Ripper
http://www.openwall.com/john/