



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;

 Game of Thrones CTF 1.0.ova

- 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



”

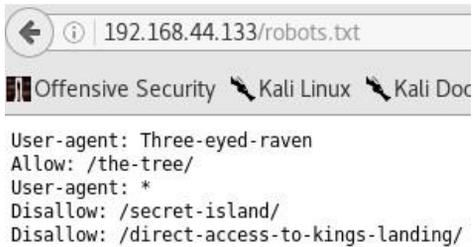
Walkthrough

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

```
root@LUCKY64:~# dirb http://192.168.44.133 /usr/share/wordlists/dirb/big.txt
-----
DIRB v2.22
By The Dark Raver
-----
START_TIME: Mon Feb 26 22:06:05 2018
URL_BASE: http://192.168.44.133/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt
-----
GENERATED WORDS: 20458
---- Scanning URL: http://192.168.44.133/ ----
=> DIRECTORY: http://192.168.44.133/css/
+ http://192.168.44.133/favicon.ico (CODE:200|SIZE:1150)
=> DIRECTORY: http://192.168.44.133/h/
=> DIRECTORY: http://192.168.44.133/imgs/
=> DIRECTORY: http://192.168.44.133/js/
=> DIRECTORY: http://192.168.44.133/music/
+ http://192.168.44.133/robots.txt (CODE:200|SIZE:135)
+ http://192.168.44.133/server-status (CODE:403|SIZE:222)
+ http://192.168.44.133/sitemap.xml (CODE:200|SIZE:214)
---- Entering directory: http://192.168.44.133/css/ ----
---- Entering directory: http://192.168.44.133/h/ ----
=> DIRECTORY: http://192.168.44.133/h/i/
---- Entering directory: http://192.168.44.133/imgs/ ----
---- Entering directory: http://192.168.44.133/js/ ----
---- Entering directory: http://192.168.44.133/music/ ----
```

Walkthrough

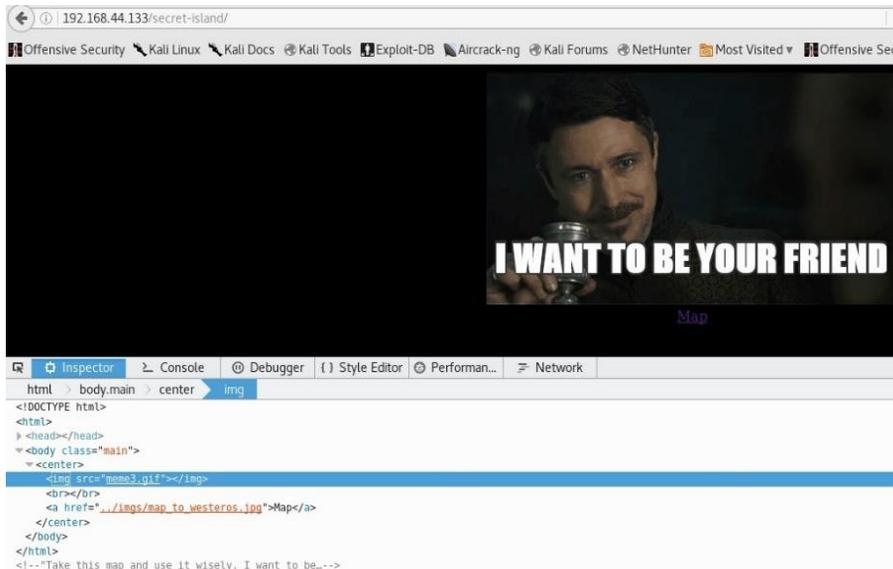
© Checking robots.txt



```
192.168.44.133/robots.txt
Offensive Security Kali Linux Kali Doc
User-agent: Three-eyed-raven
Allow: /the-tree/
User-agent: *
Disallow: /secret-island/
Disallow: /direct-access-to-kings-landing/
```

Walkthrough

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



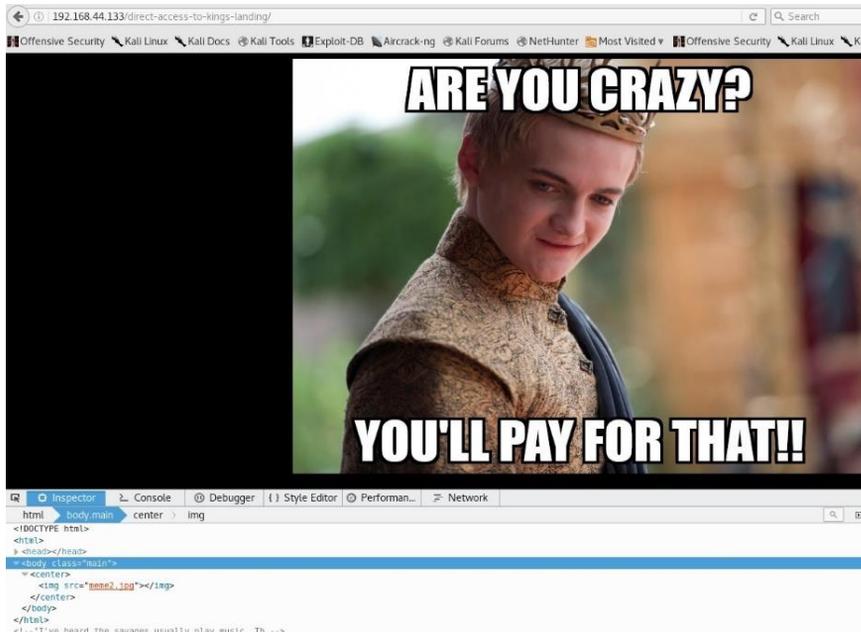
Walkthrough

© 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 accessing the server

```
root@LUCKY64:~# curl -A -iv http://192.168.44.133/the-tree/
<!DOCTYPE HTML>
<html>
  <head>
    <title>Game of Thrones CTF</title>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"/>
    <link rel="stylesheet" type="text/css" href="../css/game_of_thrones.css">
  </head>
  <body class="main">
    <center>
      
    </center>
  </body>
</html>
<!--
  "You mUSt changE your own shape and foRm if you wAnt to GEt the right aNswer from the Three-eyed raven" - Written on the tree
  by somebody
-->root@LUCKY64:~#
```

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)

```
</html>
<!--
    "I will give you three hints, I can see the future so listen carefully" - The three-eyed raven Bran Stark

    "To enter in Dorne you must identify as oberynmartell. You still should find the password"
    "3487 64535 12345 . Remember these numbers, you'll need to use them with POLITE people you'll know when to use them"
    "The savages never crossed the wall. So you must look for them before crossing it"
```

Walkthrough

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

```
--- Entering directory: http://192.168.44.133/h/i/d/d/e/ ---  
=> DIRECTORY: http://192.168.44.133/h/i/d/d/e/n/  
--- Entering directory: http://192.168.44.133/h/i/d/d/e/n/ ---  
<!--  
"My little birds are everywhere. To enter in Dorne you must say: A_verySmallManCanCastAVeryLargeShad0w. Now, you owe me" - Lord (The  
Spider) Varys  
  
"Powerful docker spells were cast over all kingdoms. We must be careful! You can't travel directly from one to another... usually. That's what the Lord of Light has shown me" - The Red Woman Melisandre  
* Connection #0 to host 192.168.44.133 left intact  
-->root@LUCKY64:~#  
root@LUCKY64:~# curl -iv http://192.168.44.133/h/i/d/d/e/n/
```

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          (?)
lg 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:~# mdecrypt -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

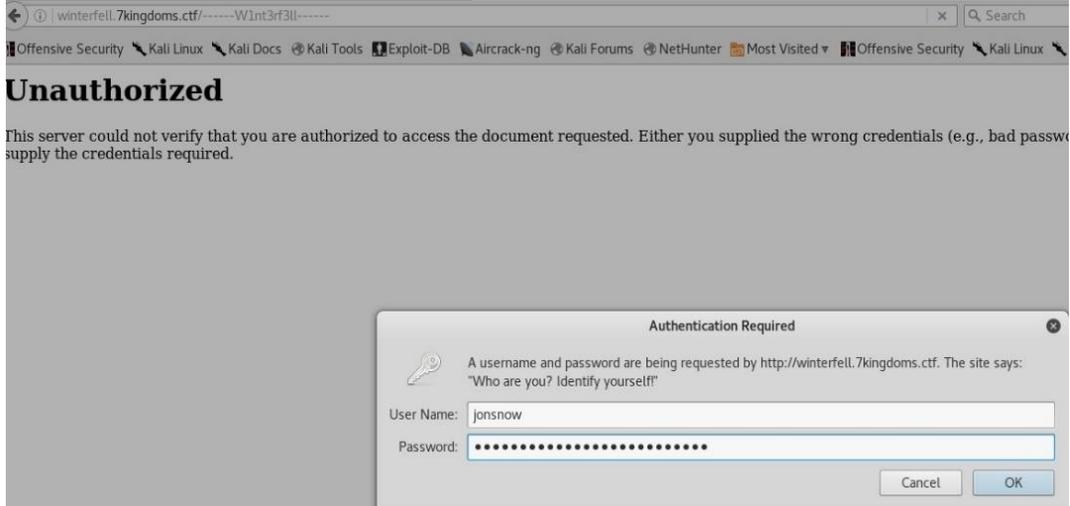
"I'll write on your map this route to get faster to Winterfell. Someday I'll be a great maester" - Samwell Tarly

http://winterfell.7kingdoms.ctf/-----W1nt3rf3ll-----
Enter using this user/pass combination:
User: jonsnow
Pass: Ha1lt0th3king1nth3n0rth!!!
```

Walkthrough

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

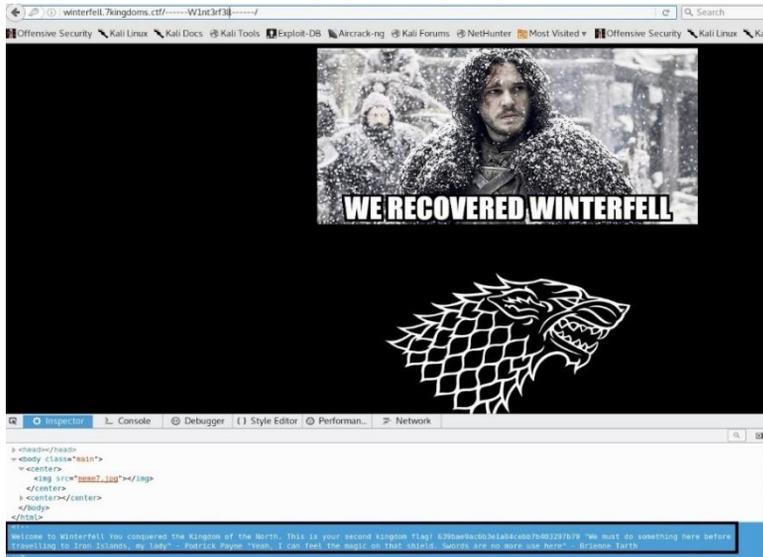
```
root@LUCKY64:~# grep --color 44.133 /etc/hosts
192.168.44.133 winterfell.7kingdoms.ctf
```



The screenshot shows a web browser window with the address bar containing `http://winterfell.7kingdoms.ctf/-----W1nt3rf3ll-----`. The browser's address bar and tabs are visible, showing various security-related sites like Kali Linux, Kali Docs, Kali Tools, Exploit-DB, Aircrack-ng, Kali Forums, NetHunter, and Most Visited. The main content area of the browser displays a large heading **Unauthorized** and a message: "This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad password) or the credentials required." In the foreground, an "Authentication Required" dialog box is open. It contains a key icon and the text: "A username and password are being requested by http://winterfell.7kingdoms.ctf. The site says: 'Who are you? Identify yourself!'" The "User Name:" field is filled with "jonsnow" and the "Password:" field is filled with a series of dots. There are "Cancel" and "OK" buttons at the bottom right of the dialog box.

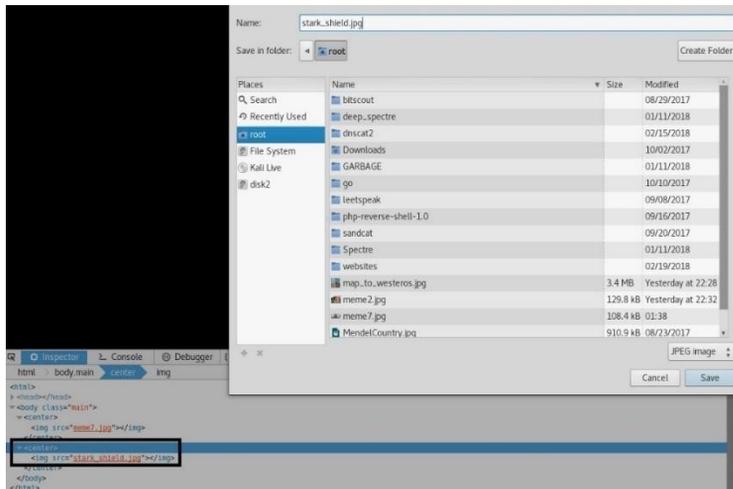
Walkthrough

© 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

```
"Timef0rconqu3rs TeXt" should be asked to enter into the Iron Islands fortress" - Theon Greyjoy  
root@LUCKY64:~#  
root@LUCKY64:~# strings stark_shield.jpg
```

Walkthrough

- © Use dig and ask for “Timef0rconqu3rs.7kingdoms.ctf” and get the third flag and obtained another username 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: 5e93dc3efa544e85dcd6311732d28f95. Now you should go to Stormlands at http://stormlands.7kingdoms.ctf:10000 . Enter using this user/pass combination: arystark/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

stormlands.7kingdoms.ctf:10000

ensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Most Visited

 STORMLANDS

Login to Stormlands

Stannis is the legitimate king!!

Username aryastark

Password

Remember login permanently?

Login Clear

Open  Wordings
~/

```
aryastark/N3ddl3_1s_a_g00d_sword#!
```

Walkthrough

© Login to stormlands.7kingdoms.ctf:10000

stormlands.7kingdoms.ctf:10000

Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Most Visited Offensive Security

Login: aryastark
Flag: ~/flag.txt
Search:

System Information
Logout

STORMLANDS

Kingdom:	Stormlands
Webmin spell version:	1.590
Processor information	Intel(R) Core(TM) i7-4910MQ CPU @ 2.90GHz, 1 cores
Running processes	0
CPU load averages	0.01 (1 min) 0.01 (5 mins) 0.00 (15 mins)
Real memory	1.44 GB total, 597.49 MB used
Virtual memory	1.47 GB total, 0 bytes used
Local disk space	41.18 GB total, 18.63 GB used
Package updates	All installed packages are up to date



Walkthrough

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

Login: anyastark
Flag: ~flag.txt
Search:
System Information
Logout

Search Webmin

Searching for a found 28 results :

Matching text	Source	Module	References
File Manager	Module name	File Manager	
Show files starting with a dot?	Configuration	File Manager	
Size of buttons in toolbar	Configuration	File Manager	
...tempt to use proper character set?	Configuration	File Manager	
...tract class files from JAR?	Configuration	File Manager	
Width for scaled images	Configuration	File Manager	
...ult archive mode for uploads	Configuration	File Manager	
Default user for uploads	Configuration	File Manager	
File extensions to edit as HTML	Configuration	File Manager	
Upload as user	User interface	File Manager	upform.cgi
Upload	User interface	File Manager	upform.cgi
Failed to write to : .	User interface	File Manager	upload.cgi upload2.cgi
...user does not support java	User interface	File Manager	File Manager
File to upload	User interface	File Manager	upform.cgi
Return to Webmin index.	User interface	File Manager	File Manager
No file selected to upload.	User interface	File Manager	upload.cgi
Filename:	User interface	File Manager	edit_html.cgi
Change upload to a symbolic link	User interface	File Manager	upload.cgi
... Are you sure that you want to overwrite it?	User interface	File Manager	upload.cgi
Upload to directory	User interface	File Manager	upform.cgi
Uncompress ZIP or TAR file?	User interface	File Manager	upform.cgi
Upload directory does not exist...	User interface	File Manager	upload.cgi
...ou are not allowed to create	User interface	File Manager	upload.cgi upload2.cgi
Create HTML file	User interface	File Manager	edit_html.cgi
Switch to plain text mode	User interface	File Manager	edit_html.cgi
Upload File	User interface	File Manager	upform.cgi
Save and Close	User interface	File Manager	edit_html.cgi
File Manager	User interface	File Manager	File Manager

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/>