Cyber Security – An Offensive Mindset Report

HackTheBox – Curling

Introduction

4 weeks study in the studio was really a hard time for me as a noob in cyber security that everything in cyber filed need to do more effort on it. However, I really enjoyed the life like that an efficient communication and knowledge sharing to those lovely buddies and tight time management life-style. All the effort is to prepare for virtual machine challenge. This is my first time try to get one virtual machine and special thank you Darshil Shah who helped me a lot for every stuck step by step. Curling is more like a real-life challenge that combined vulnerable website and CTF tricks. This report will show the walkthrough of Curling box.

Objective

The primary objective is to learn cyber security by attacking virtual box under a legal environment. There are many possible vulnerabilities which may cause malicious hacking, such as: data leak, property loss, data loss and website crush down. By finding those vulnerabilities to improve our security skills.

Tools

Here are the environment/tools that used below.

Environment:

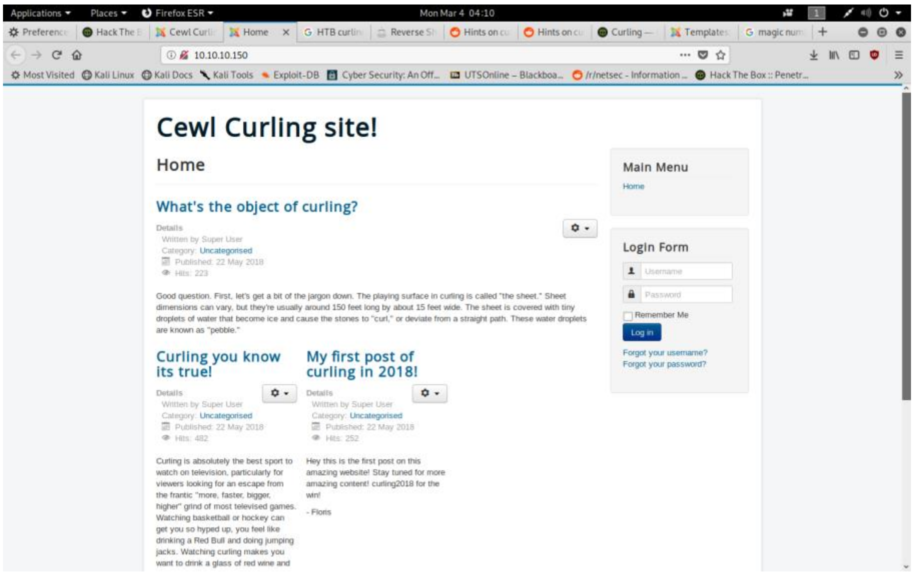
Kali Linux System (the best Linux system for hacker)
Access to HackTheBox VPN

Tools:
Nmap
Dirb
Burpsuite
CyberChef
php-reverse-shell (by pentestmonkey@pentestmonkey.net)

Intelligence Gathering

0. Get VM’S IP

The box already gives the IP address 10.10.10.150, visit it through browser will see the Curling page.



Cewl Curling site!

Home

What's the object of curling?

Details
Written by Super User
Category: Uncategorised
Published: 22 May 2018
Hits: 223

Good question. First, let's get a bit of the jargon down. The playing surface in curling is called "the sheet." Sheet dimensions can vary, but they're usually around 150 feet long by about 15 feet wide. The sheet is covered with tiny droplets of water that become ice and cause the stones to "curl," or deviate from a straight path. These water droplets are known as "pebble."

Curling you know its true!

Details
Written by Super User
Category: Uncategorised
Published: 22 May 2018
Hits: 482

Curling is absolutely the best sport to watch on television, particularly for viewers looking for an escape from the frantic "more, faster, bigger, higher" grind of most televised games. Watching basketball or hockey can get you so hyped up, you feel like drinking a Red Bull and doing jumping jacks. Watching curling makes you want to drink a glass of red wine and

My first post of curling in 2018!

Details
Written by Super User
Category: Uncategorised
Published: 22 May 2018
Hits: 252

Hey this is the first post on this amazing website! Stay tuned for more amazing content! curling2018 for the win!

- Floris

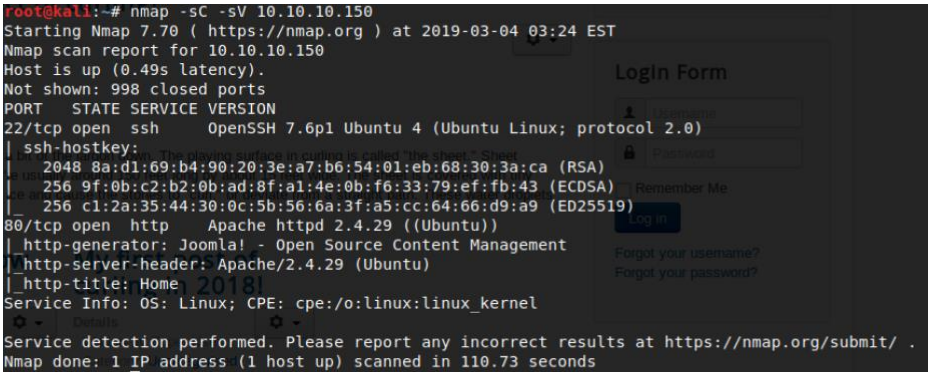
Main Menu
Home

Login Form
Username
Password
□ Remember Me
Log in
Forgot your username?
Forgot your password?

In the homepage, there is a login system, and some articles. There are more clues hide in source code, come back to it later.

1. Enumeration

Then, try to find any open ports by using Nmap.



```
root@kali:~# nmap -sC -sV 10.10.10.150
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-04 03:24 EST
Nmap scan report for 10.10.10.150
Host is up (0.49s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8a:d1:69:b4:90:20:3e:a7:b6:54:01:eb:68:30:3a:ca (RSA)
|   256 9f:0b:c2:b2:0b:ad:8f:a1:4e:0b:f6:33:79:ef:fb:43 (ECDSA)
|_  256 c1:2a:35:44:30:0c:5b:56:6a:3f:a5:cc:64:66:d9:a9 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Joomla! - Open Source Content Management
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Home
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 110.73 seconds
```

Open terminal and code: nmap -sC -sV 10.10.10.150

There are two ports opened: Port 22 – ssh, and Port 80 – http.

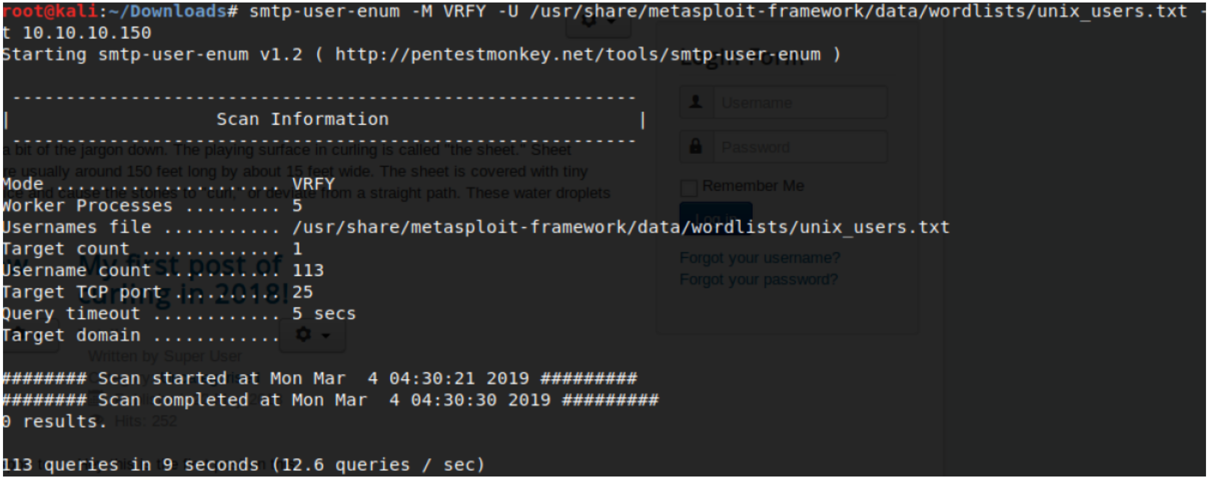
HTTP is the port that server "listens to" or expects to receive from a Web client, assuming that the default was taken when the server was configured or set up. So that access the website at port 80.

1.1 Services enumeration

nmap -p- -sS -A 10.10.10.150

1.2 Users enumeration

smtp-user-enum -M VRFY -U /usr/share/metasploit-framework/data/wordlists/unix_users.txt -t 10.10.10.150

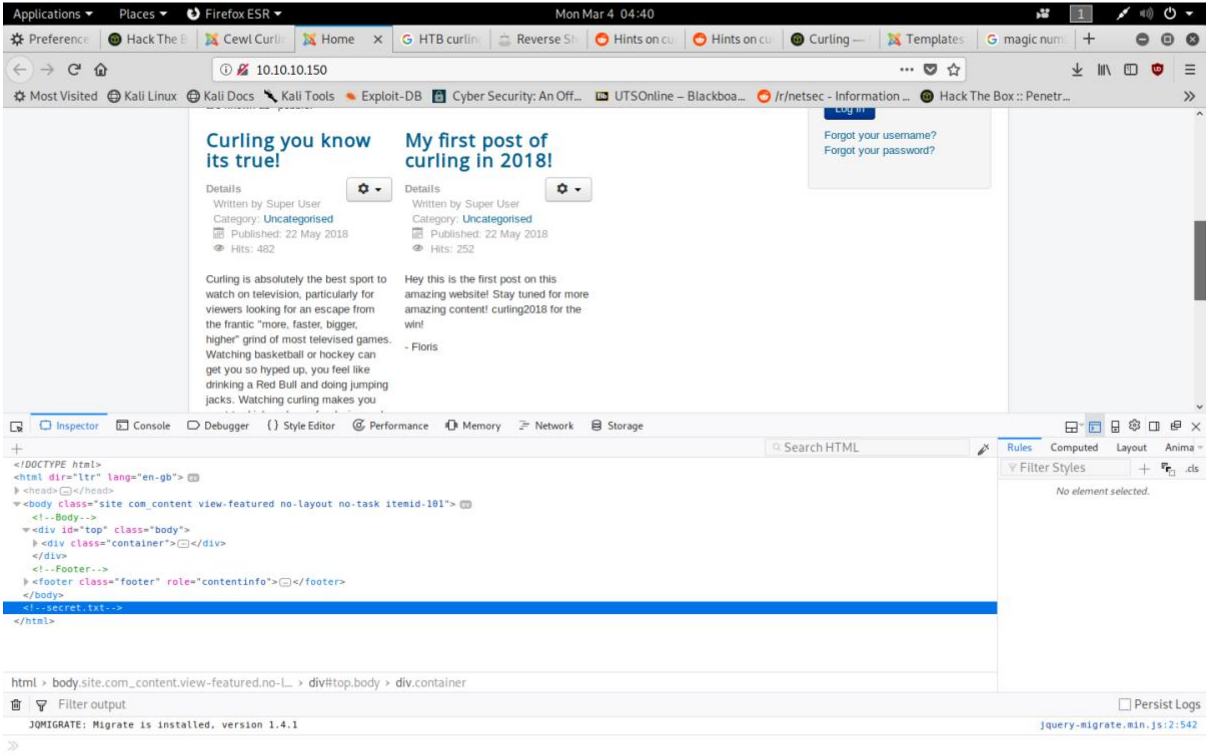


```
root@kali:~/Downloads# smtp-user-enum -M VRFY -U /usr/share/metasploit-framework/data/wordlists/unix_users.txt -
t 10.10.10.150
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Usernames file ........... /usr/share/metasploit-framework/data/wordlists/unix_users.txt
Target count ............. 1
Username count ........... 113
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Mon Mar  4 04:30:21 2019 #########
######## Scan completed at Mon Mar  4 04:30:30 2019 #########
0 results.

113 queries in 9 seconds (12.6 queries / sec)
```

2. Gaining Access

2.1 View the source code (find the password)

Open developer tool, view the source code, an obvious comment <!—secret.txt--> stand there. It must be a .txt file in this website, so have a try with .txt file.



Curling you know its true!

Details
Written by Super User
Category: Uncategorised
Published: 22 May 2018
Hits: 482

Curling is absolutely the best sport to watch on television, particularly for viewers looking for an escape from the frantic "more, faster, bigger, higher" grind of most televised games. Watching basketball or hockey can get you so hyped up, you feel like drinking a Red Bull and doing jumping jacks. Watching curling makes you

My first post of curling in 2018!

Details
Written by Super User
Category: Uncategorised
Published: 22 May 2018
Hits: 252

Hey this is the first post on this amazing website! Stay tuned for more amazing content! curling2018 for the win!

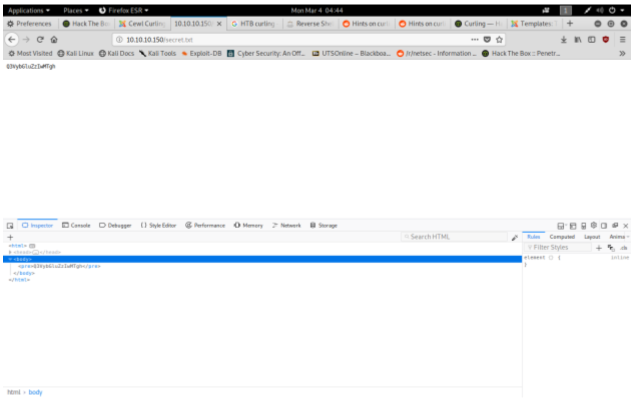
- Floris

```
<!DOCTYPE html>
<html dir="ltr" lang="en-gb">
 <head>…</head>
 <body class="site com_content view-featured no-layout no-task itemid-101">
   <!--Body-->
  <div id="top" class="body">
    <div class="container">…</div>
   </div>
   <!--Footer-->
  <footer class="footer" role="contentinfo">…</footer>
  </body>
  <!--secret.txt-->
</html>
```

html › body.site.com_content.view-featured.no-l... › div#top.body › div.container

```
JQMIGRATE: Migrate is installed, version 1.4.1          jquery-migrate.min.js:2:542
```

Wow, in the page http://10.10.10.150/secret.txt , only shows a string which looks encoded by base64.

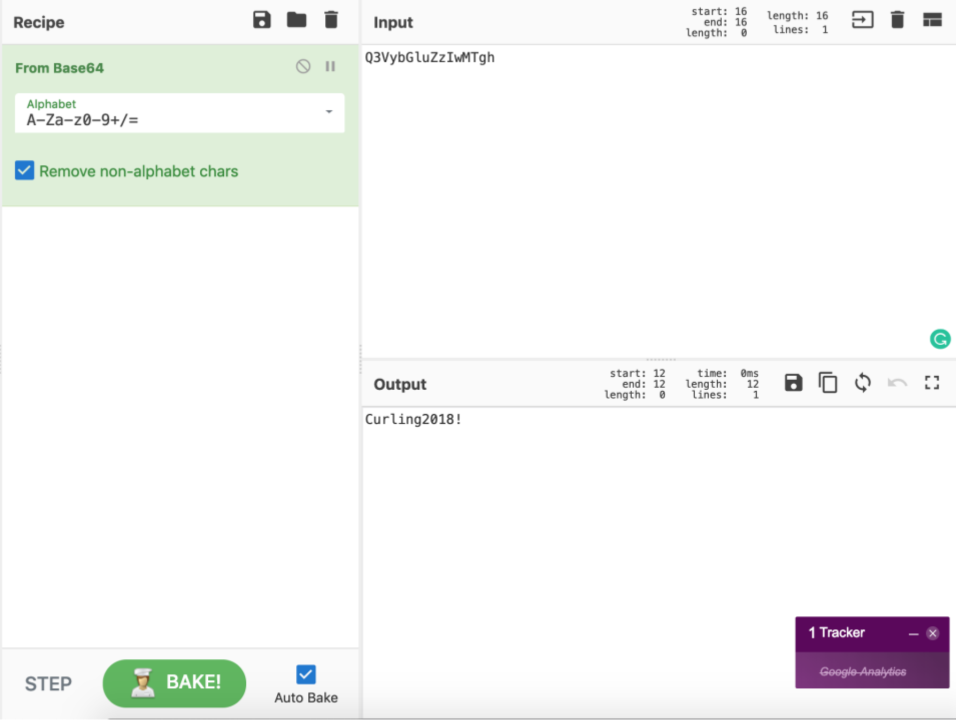


10.10.10.150/secret.txt

```
Q3VybGluZzIwMTgh
```

```
<html>
<head></head>
<body>
  <pre>Q3VybGluZzIwMTgh</pre>
</body>
</html>
```

Then, using CyberChef decode this string.



Recipe: From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

Input

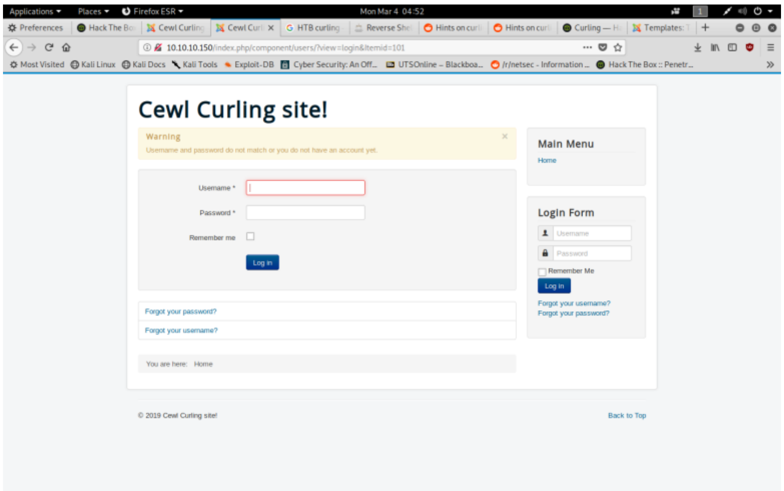
```
Q3VybGluZzIwMTgh
```

Output

```
Curling2018!
```

It must be a login password – “Curling2018!”

Try the password with random username



10.10.10.150/index.php/component/users/?view=login&Itemid=101

Cewl Curling site!

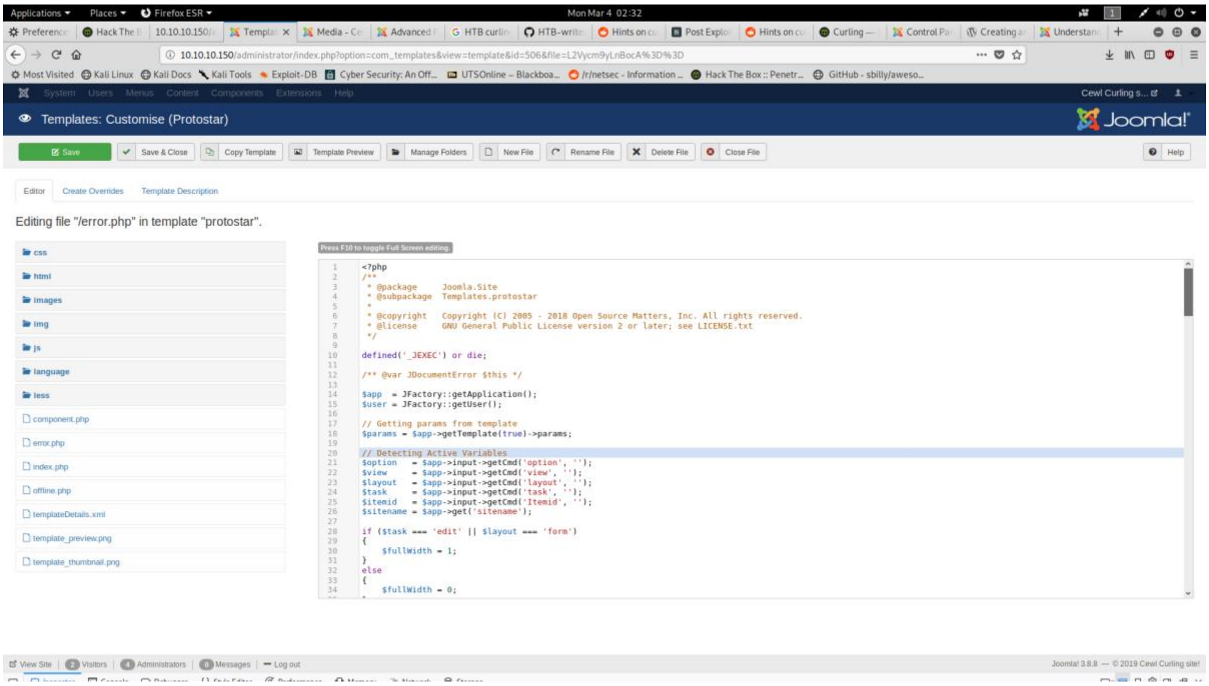
Warning
Username and password do not match or you do not have an account yet.

Username *

Password *

Remember me □

This is a smart error that user do not know neither username or the password is wrong.



Editing file "/error.php" in template "protostar".

```
<?php
/**
 * @package     Joomla.Site
 * @subpackage  Templates.protostar
 *
 * @copyright   Copyright (C) 2005 - 2018 Open Source Matters, Inc. All rights reserved.
 * @license     GNU General Public License version 2 or later; see LICENSE.txt
 */

defined('_JEXEC') or die;

/** @var JDocumentError $this */

$app  = JFactory::getApplication();
$user = JFactory::getUser();

// Getting params from template
$params = $app->getTemplate(true)->params;

// Detecting Active Variables
$option   = $app->input->getCmd('option', '');
$view     = $app->input->getCmd('view', '');
$layout   = $app->input->getCmd('layout', '');
$task     = $app->input->getCmd('task', '');
$itemid   = $app->input->getCmd('Itemid', '');
$sitename = $app->get('sitename');

if ($task === 'edit' || $layout === 'form')
{
    $fullWidth = 1;
}
else
{
    $fullWidth = 0;
```