# Challenge: An unusual sighting

## Challenge Description :

As the preparations come to an end, and The Fray draws near each day, our newly established team has started work on refactoring the new CMS application for the competition. However, after some time we noticed that a lot of our work mysteriously has been disappearing! We managed to extract the SSH Logs and the Bash History from our dev server in question. The faction that manages to uncover the perpetrator will have a massive bonus come the competition! Note: Operating Hours of Korp: 0900 - 1900

## Context :

- We are given a questionnaire, based upon a bash_history.txt file and a sshd.log file. You will need to go through both and answer the question based on the log files.

## Flag :

- First Install the PcaP file and open it up with Wireshark, the first thing you will notice is that it's not a normal looking TCP steam or http requests packets its Modbus packets.

```
What is the IP Address and Port of the SSH Server (IP:PORT)
> 100.107.36.130:2221
[+] Correct!

What time is the first successful Login
> 2024-02-13 11:29:50
[+] Correct!

What is the time of the unusual Login
> 2024-02-19 04:00:14
[+] Correct!

What is the Fingerprint of the attacker's public key
> OPkBSs6okUKraq8pYo4XwwBg55QSo210F09FCe1-yj4
[+] Correct!

What is the first command the attacker executed after logging in
> whoami
[+] Correct!

What is the final command the attacker executed before logging out
> ./setup
[+] Correct!

[+] Here is the flag: HTB{4n_unusual_s1ght1ng_1n_SSH_l0gs!}
```

The Flag : HTB{4n_unusual_s1ght1ng_1n_SSH_l0gs!}