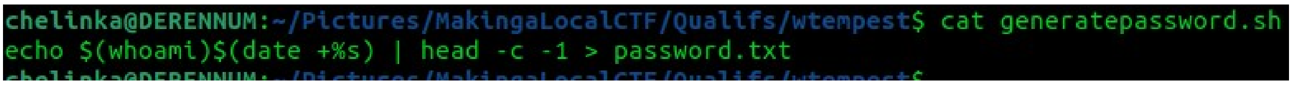
Cloudy Wtmp a chance of meatballs

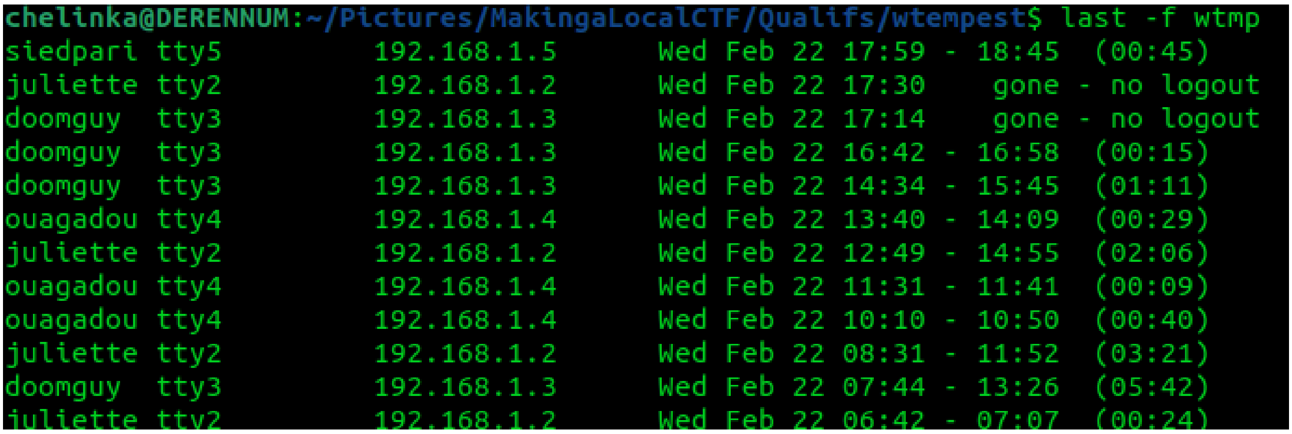
For this challenge, we were given a wtmp file, a small script in bash and a password-protected zip containing the flag.

The script is pretty straightforward, as it consists of just the username concatenated the timestamp, down to the second, when the command was run.



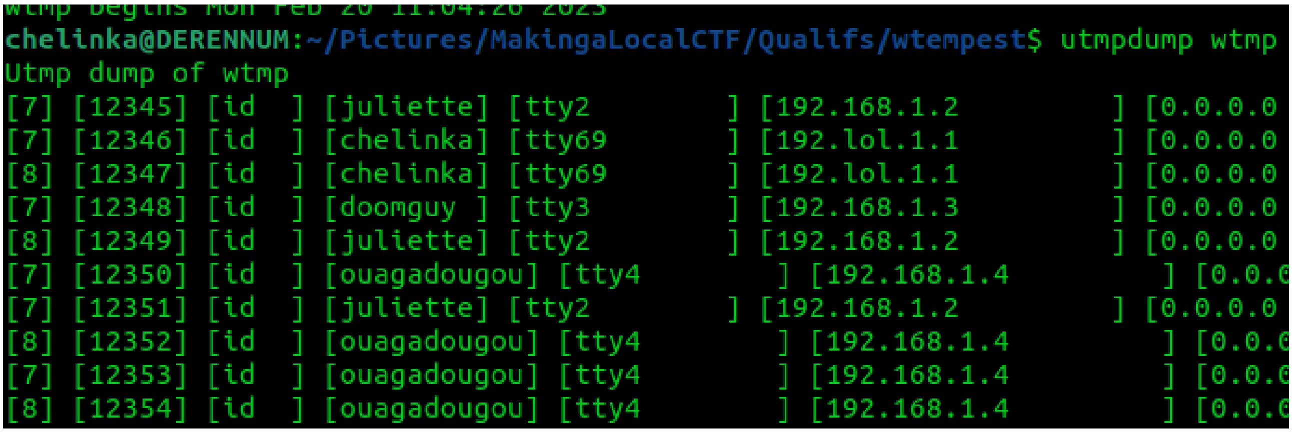
```
chelinka@DERENNUM:~/Pictures/MakingaLocalCTF/Qualifs/wtempest$ cat generatepassword.sh
echo $(whoami)$(date +%s) | head -c -1 > password.txt
chelinka@DERENNUM:~/Pictures/MakingaLocalCTF/Qualifs/wtempest$
```

By using the command last, we can see the content of the wtmp file:



```
chelinka@DERENNUM:~/Pictures/MakingaLocalCTF/Qualifs/wtempest$ last -f wtmp
siedpari tty5         192.168.1.5      Wed Feb 22 17:59 - 18:45  (00:45)
juliette tty2         192.168.1.2      Wed Feb 22 17:30    gone - no logout
doomguy  tty3         192.168.1.3      Wed Feb 22 17:14    gone - no logout
doomguy  tty3         192.168.1.3      Wed Feb 22 16:42 - 16:58  (00:15)
doomguy  tty3         192.168.1.3      Wed Feb 22 14:34 - 15:45  (01:11)
ouagadou tty4         192.168.1.4      Wed Feb 22 13:40 - 14:09  (00:29)
juliette tty2         192.168.1.2      Wed Feb 22 12:49 - 14:55  (02:06)
ouagadou tty4         192.168.1.4      Wed Feb 22 11:31 - 11:41  (00:09)
ouagadou tty4         192.168.1.4      Wed Feb 22 10:10 - 10:50  (00:40)
juliette tty2         192.168.1.2      Wed Feb 22 08:31 - 11:52  (03:21)
doomguy  tty3         192.168.1.3      Wed Feb 22 07:44 - 13:26  (05:42)
juliette tty2         192.168.1.2      Wed Feb 22 06:42 - 07:07  (00:24)
```

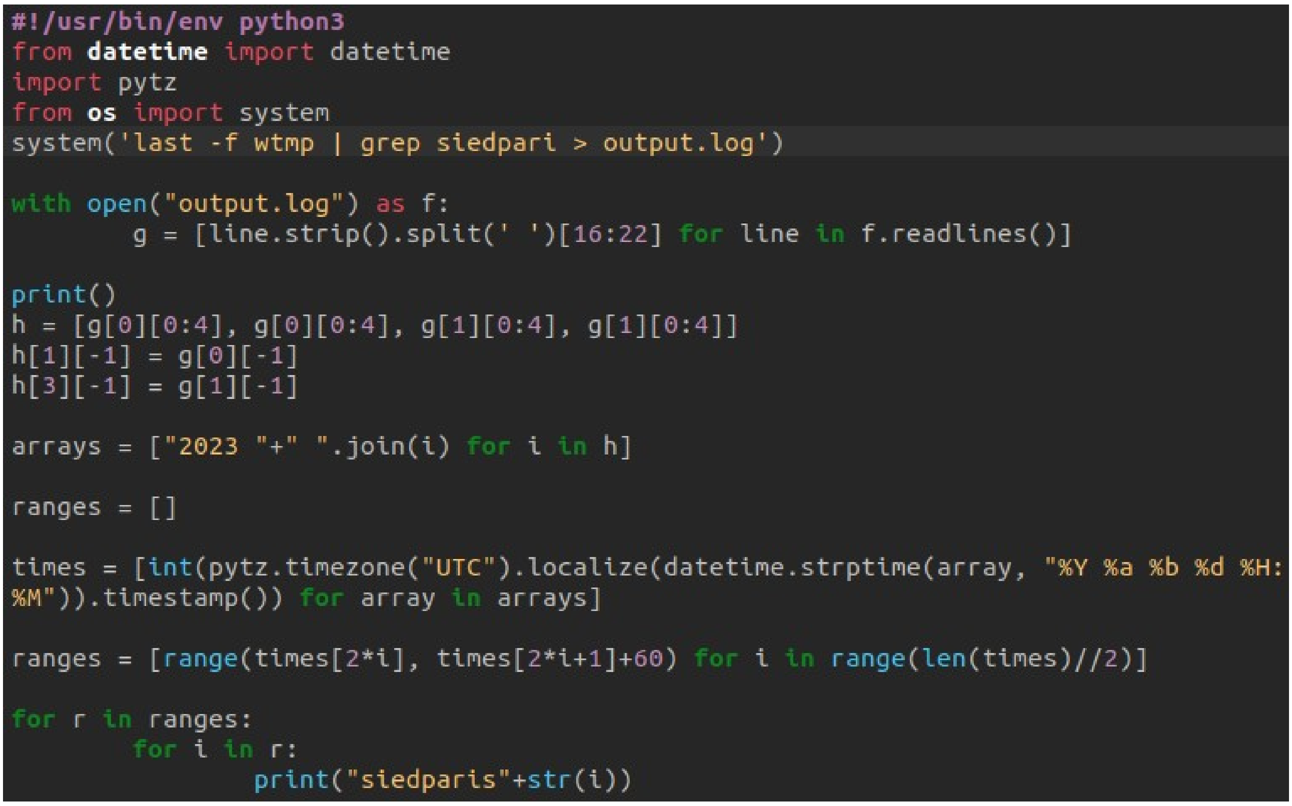
The file contains the user credentials, as well as the time ranges at which they were logged in. The usernames are truncated after the eight character, but we can extract the full name with `utmpdump`, or by reading the lore.



```
wtmp begins Mon Feb 20 11:04:20 2023
chelinka@DERENNUM:~/Pictures/MakingaLocalCTF/Qualifs/wtempest$ utmpdump wtmp
Utmp dump of wtmp
[7] [12345] [id  ] [juliette] [tty2         ] [192.168.1.2         ] [0.0.0.0
[7] [12346] [id  ] [chelinka] [tty69        ] [192.lol.1.1         ] [0.0.0.0
[8] [12347] [id  ] [chelinka] [tty69        ] [192.lol.1.1         ] [0.0.0.0
[7] [12348] [id  ] [doomguy ] [tty3         ] [192.168.1.3         ] [0.0.0.0
[8] [12349] [id  ] [juliette] [tty2         ] [192.168.1.2         ] [0.0.0.0
[7] [12350] [id  ] [ouagadougou] [tty4         ] [192.168.1.4         ] [0.0.0
[7] [12351] [id  ] [juliette] [tty2         ] [192.168.1.2         ] [0.0.0.0
[8] [12352] [id  ] [ouagadougou] [tty4         ] [192.168.1.4         ] [0.0.0
[7] [12353] [id  ] [ouagadougou] [tty4         ] [192.168.1.4         ] [0.0.0
[8] [12354] [id  ] [ouagadougou] [tty4         ] [192.168.1.4         ] [0.0.0
```

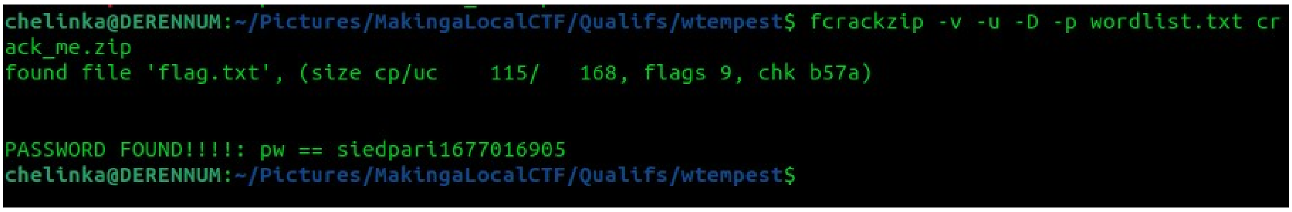
From this, we can easily recover the password. Taking into account that the time is in UTC, we can generate a wordlist with which we can break the zip file’s security.

This python script opens the wtmp file into output.log before reading the entries corresponding to the user “siedparis”, which is the fishy user, and prints out the wordlist.



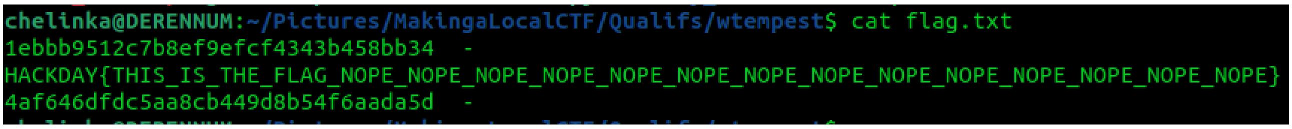
```
#!/usr/bin/env python3
from datetime import datetime
import pytz
from os import system
system('last -f wtmp | grep siedpari > output.log')

with open("output.log") as f:
        g = [line.strip().split(' ')[16:22] for line in f.readlines()]

print()
h = [g[0][0:4], g[0][0:4], g[1][0:4], g[1][0:4]]
h[1][-1] = g[0][-1]
h[3][-1] = g[1][-1]

arrays = ["2023 "+" ".join(i) for i in h]

ranges = []

times = [int(pytz.timezone("UTC").localize(datetime.strptime(array, "%Y %a %b %d %H:
%M")).timestamp()) for array in arrays]

ranges = [range(times[2*i], times[2*i+1]+60) for i in range(len(times)//2)]

for r in ranges:
        for i in r:
                print("siedparis"+str(i))
```

After this, we just need to user a bruteforcing tool such as fcrackzip and give him the wordlist and the zip file and voilà:



```
chelinka@DERENNUM:~/Pictures/MakingaLocalCTF/Qualifs/wtempest$ fcrackzip -v -u -D -p wordlist.txt cr
ack_me.zip
found file 'flag.txt', (size cp/uc    115/   168, flags 9, chk b57a)


PASSWORD FOUND!!!!: pw == siedpari1677016905
chelinka@DERENNUM:~/Pictures/MakingaLocalCTF/Qualifs/wtempest$
```

The only thing left to do is to extract then print the flag:



```
chelinka@DERENNUM:~/Pictures/MakingaLocalCTF/Qualifs/wtempest$ cat flag.txt
1ebbb9512c7b8ef9efcf4343b458bb34  -
HACKDAY{THIS_IS_THE_FLAG_NOPE_NOPE_NOPE_NOPE_NOPE_NOPE_NOPE_NOPE_NOPE_NOPE_NOPE_NOPE_NOPE_NOPE_NOPE}
4af646dfdc5aa8cb449d8b54f6aada5d  -
```

FLAG:
HACKDAY{THIS_IS_THE_FLAG_NOPE_NOPE_NOPE_NOPE_NOPE_NOPE_NOPE_NOPE_NOPE_NOPE_NOPE_NOPE_NOPE_NOPE_NOPE}

Written by Chelinka, 22 March 2023