Stolen Password

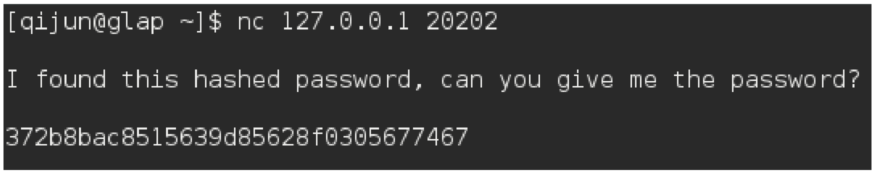
Problem: Can you crack a password for me, if I can log on I will give you the flag.

Given: nc 127.0.0.1 20202

Hints: Luckily these 5 MaD people weren't salty.

Steps:

(1) We connect to the service. We get a hex string “372b8bac8515639d85628f0305677467”. Since the password is stolen, the string could be the hash or the encryption of the password. The hint states “5 MaD” which implies MD5. The hint also indicates the hash is not salted. Hence, the string could be an unsalted MD5 hash of the password.



```
[qijun@glap ~]$ nc 127.0.0.1 20202

I found this hashed password, can you give me the password?

372b8bac8515639d85628f0305677467
```

(2) We need to reverse the hash to the password. Theoretically, it is not possible to reverse a secure hash. But, MD5 is a weak hash now and there are many online MD5 reverse lookup tools. So, let's try one http://md5decrypt.net/ to get the password and the flag...