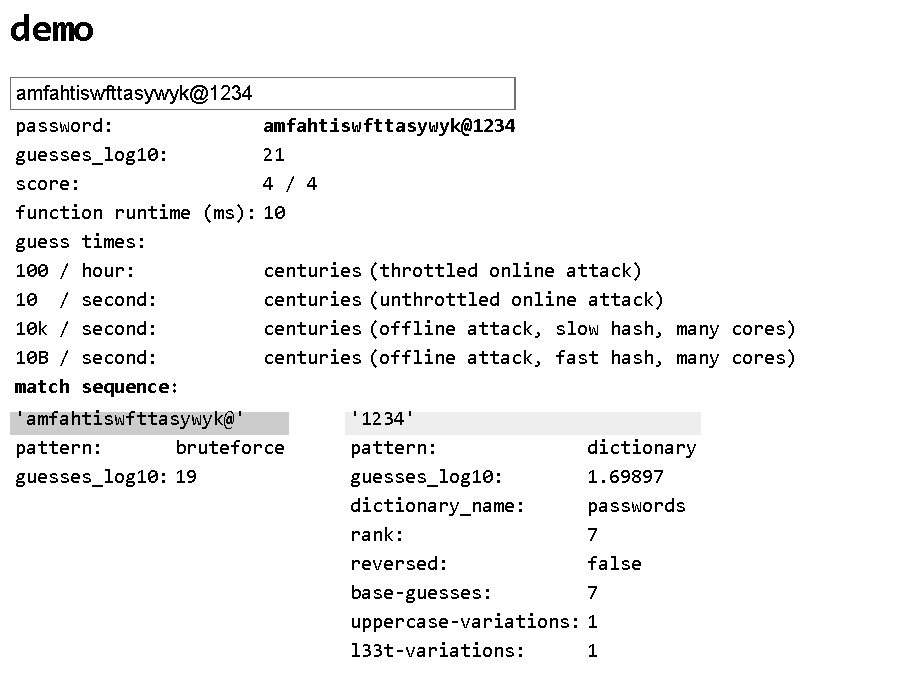
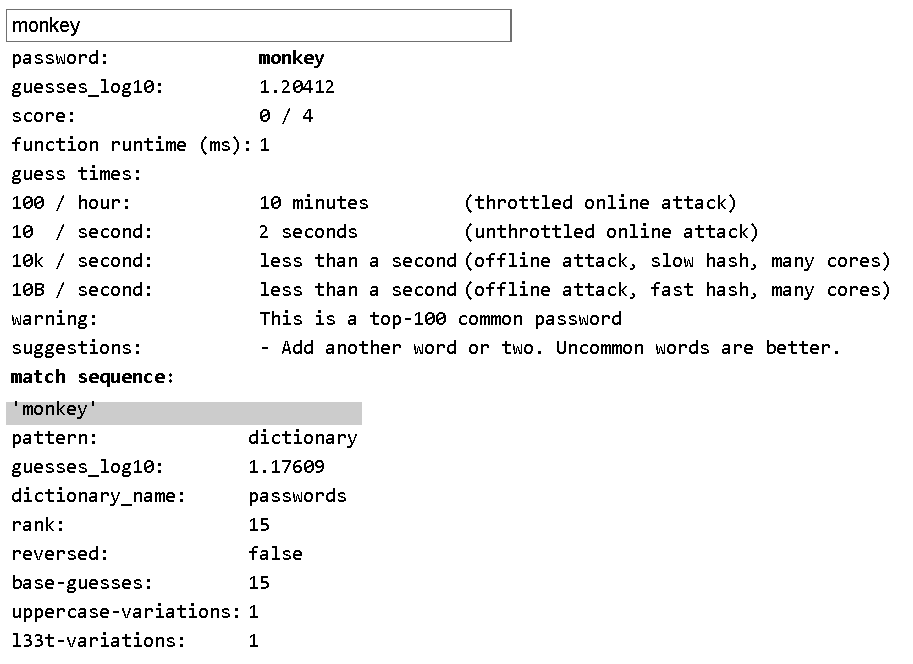
|  |  |
| --- | --- |
| **Name** | Adit Verma |
| **Roll Number** | K062 |

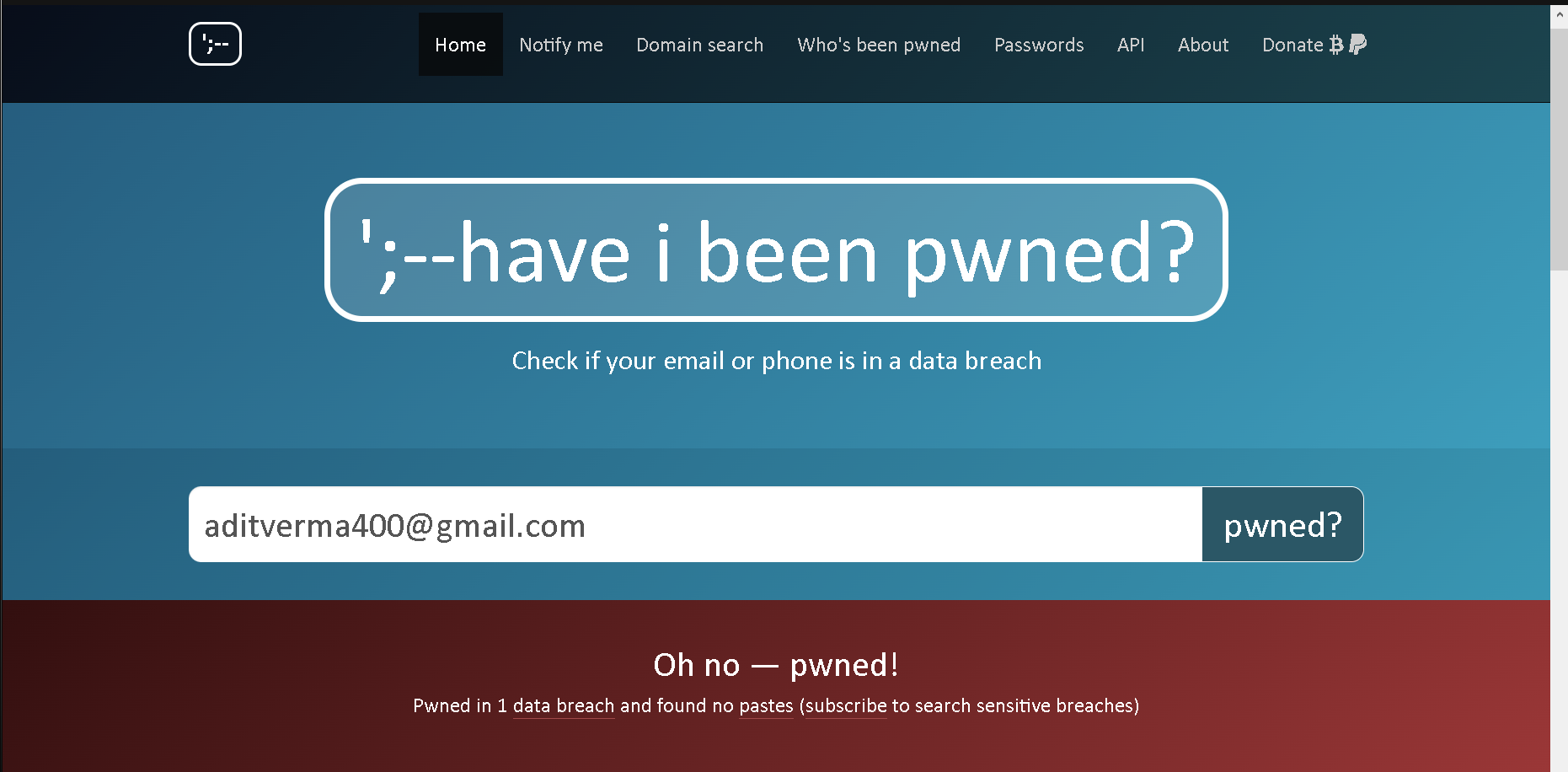
**Screenshots**

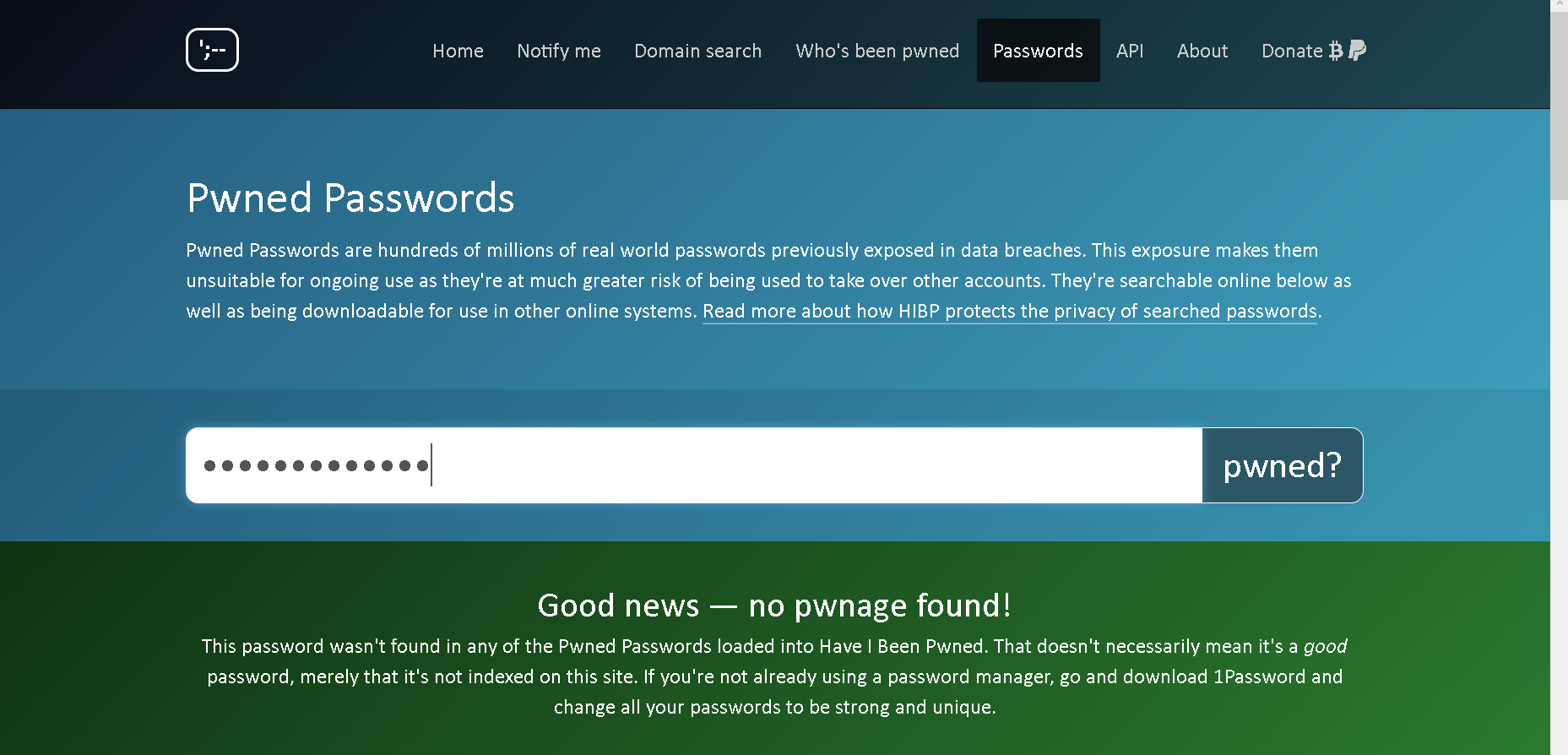
1. **Testing the strength of passwords**



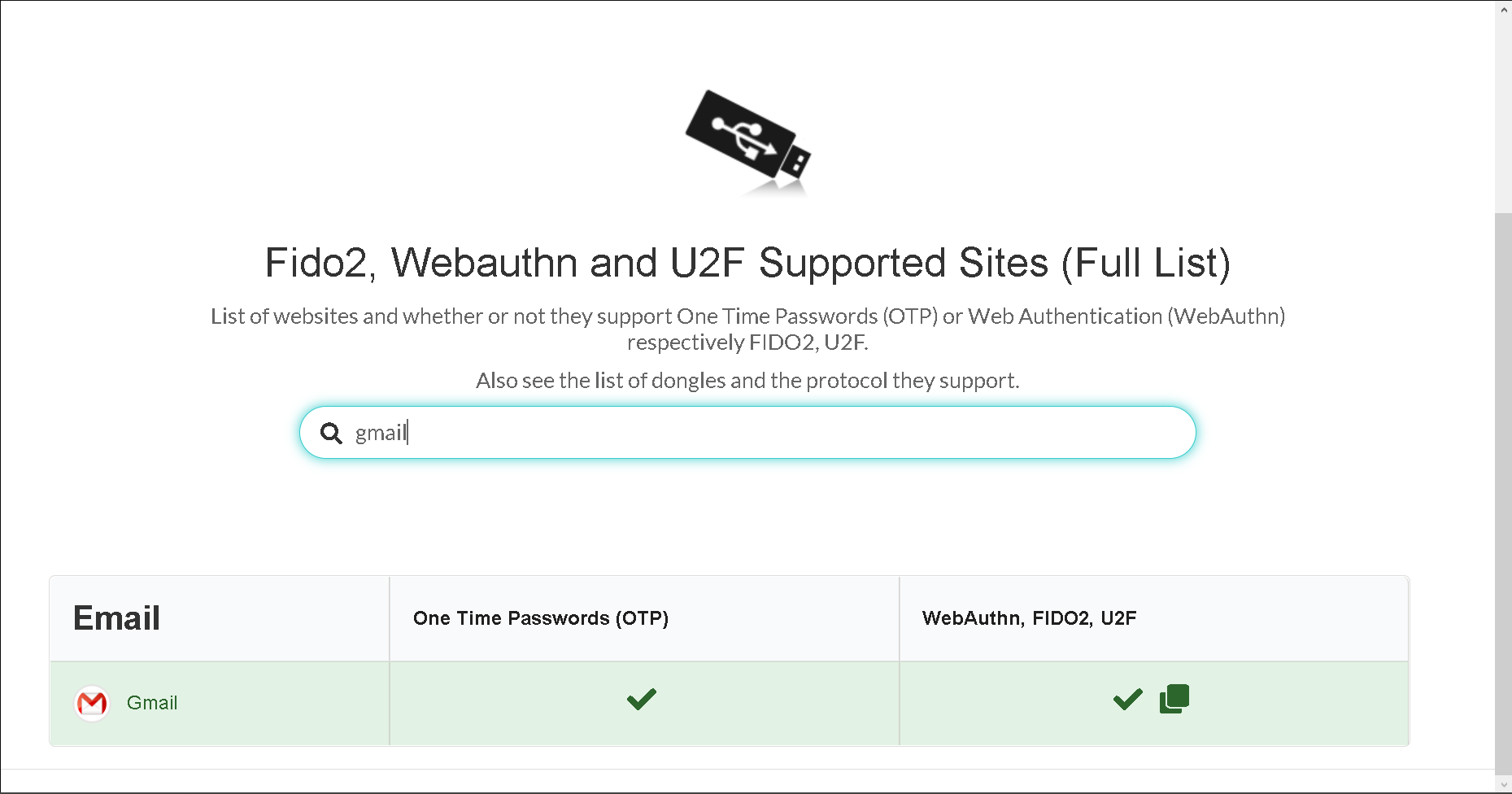


1. **Checking if my online accounts have been pwned**

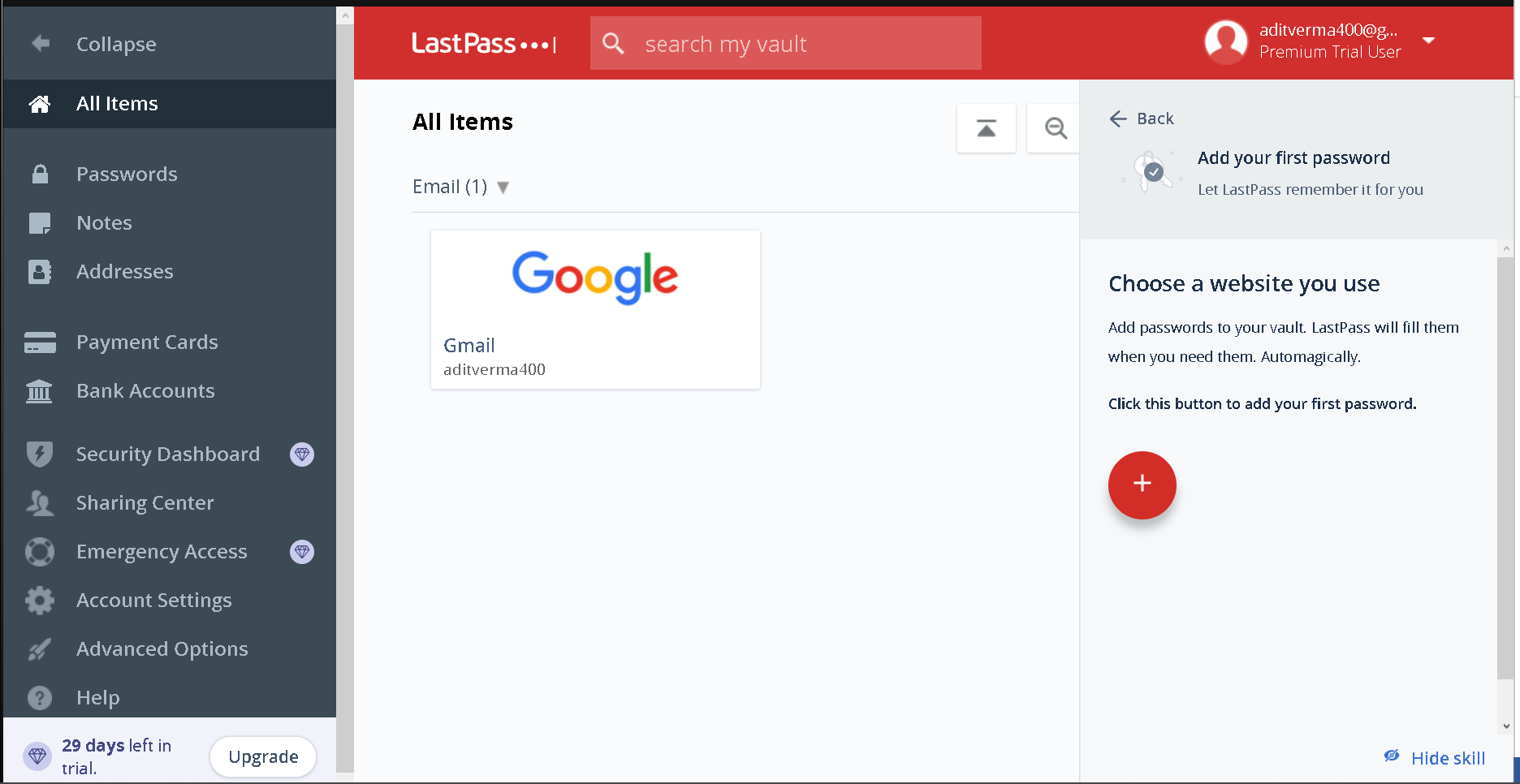




1. **Checking if the services that I use have 2fa**

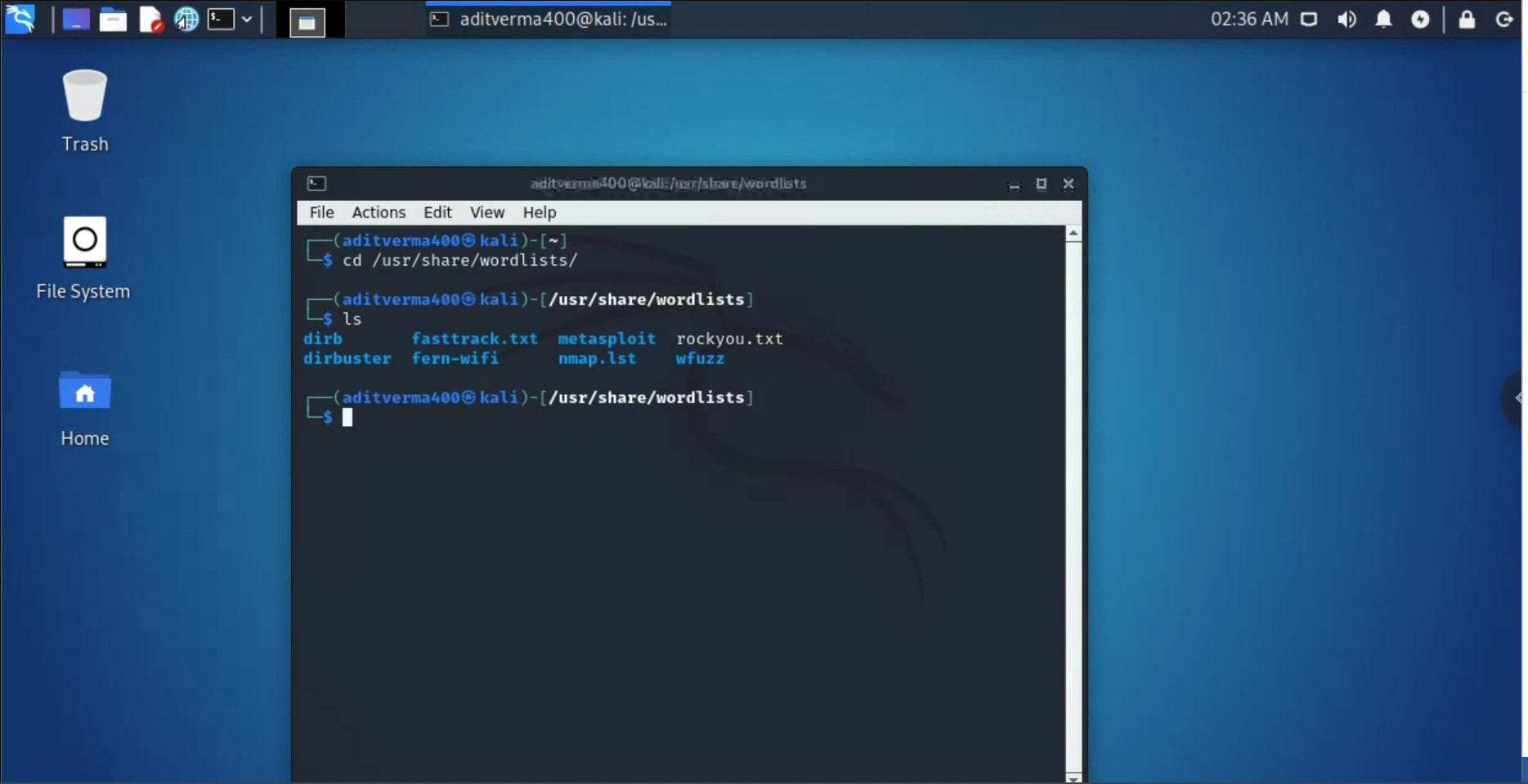


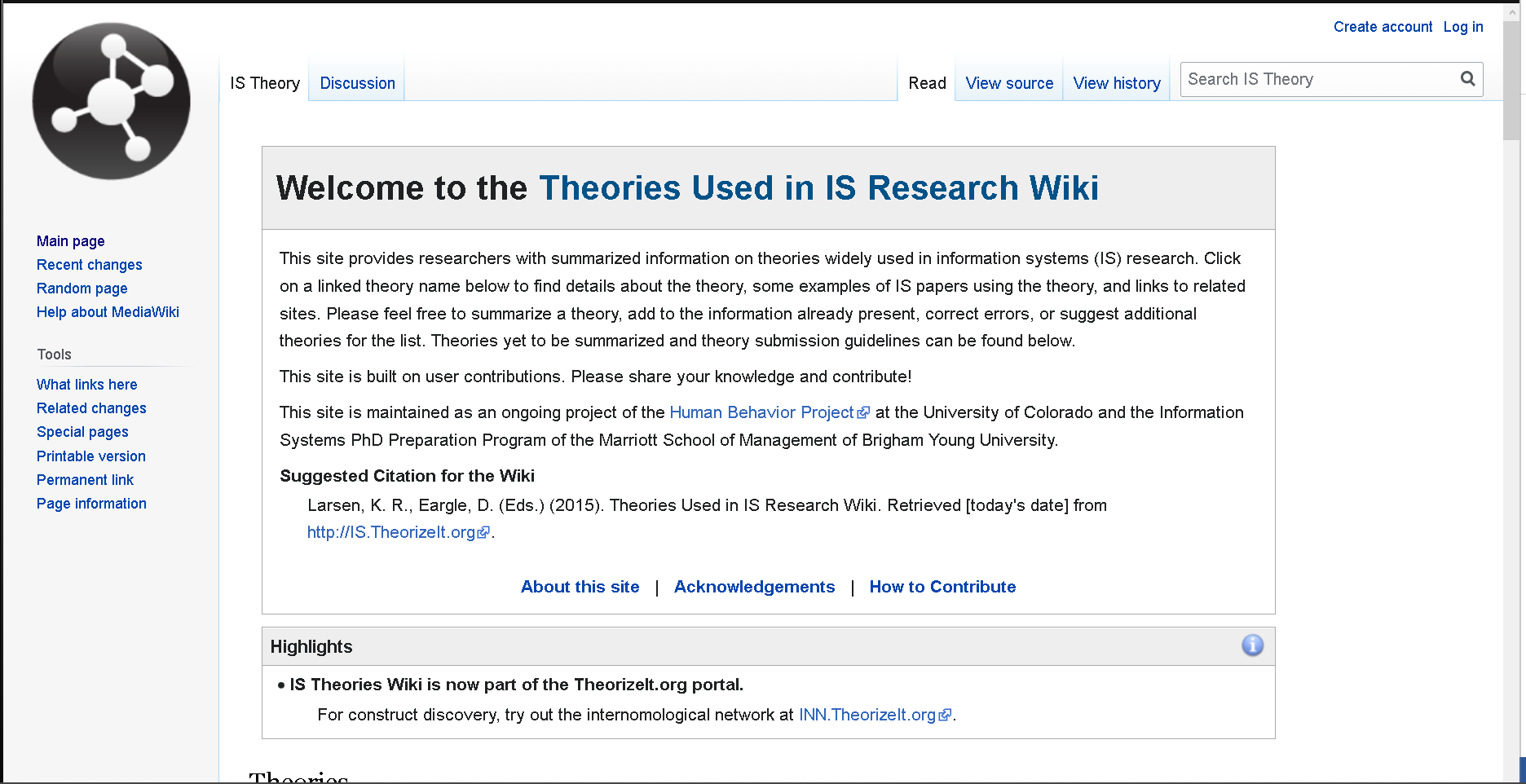
1. **Screenshot of Password Manager**

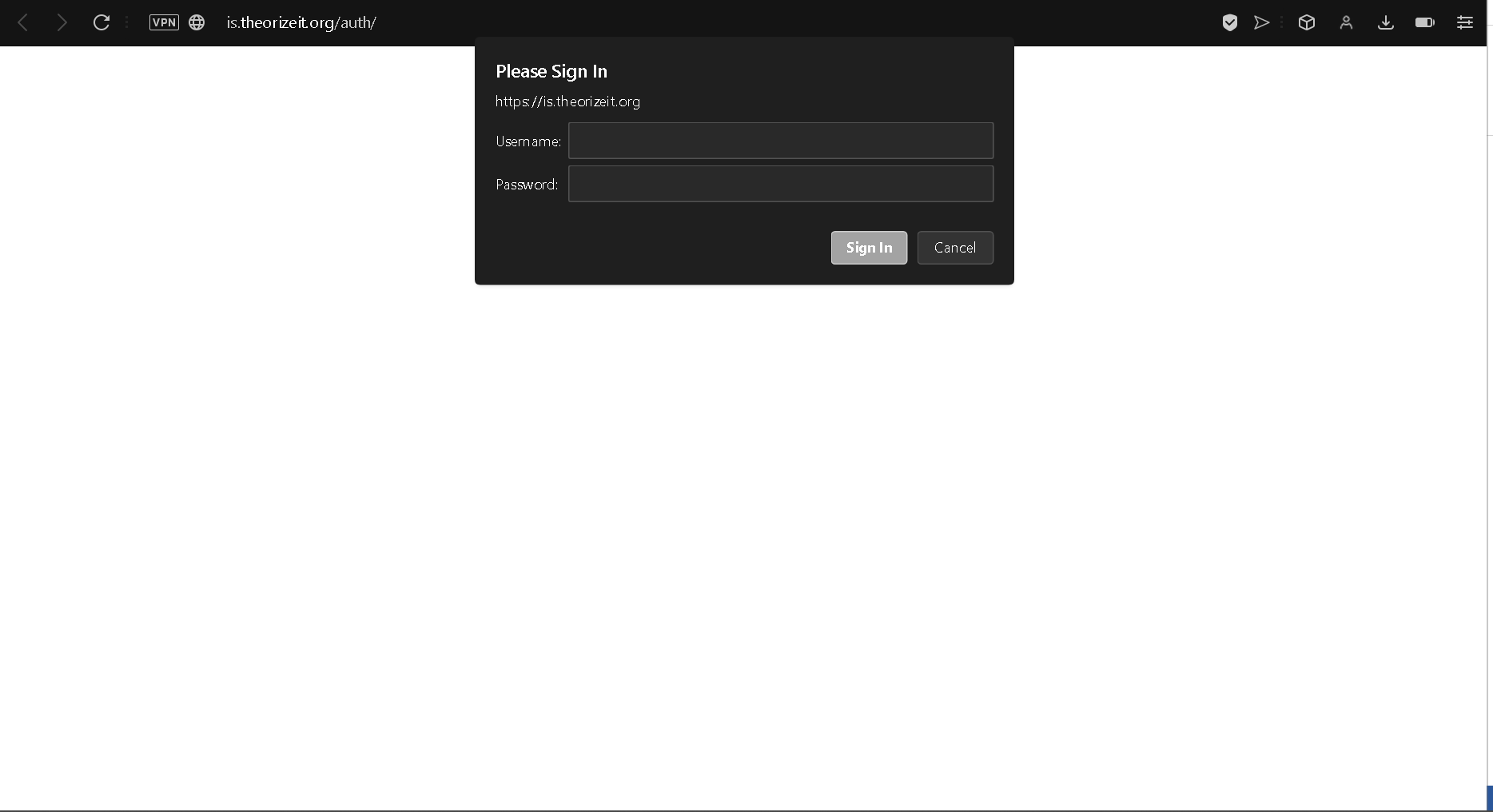


1. **Password Cracking**

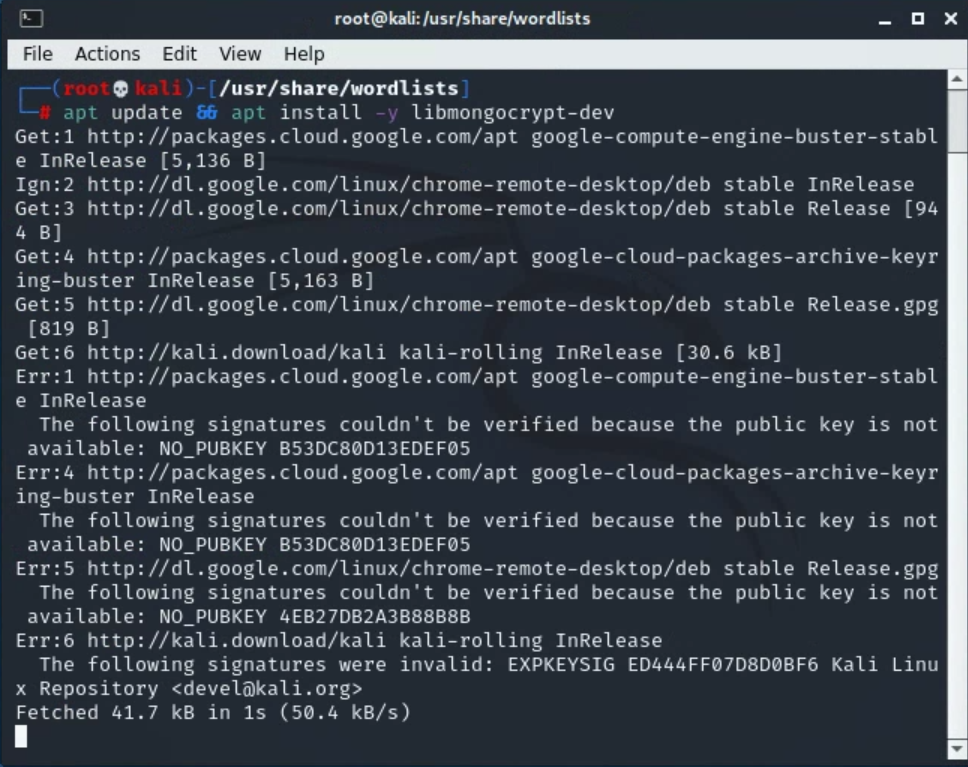
Unzipping rockyou.txt



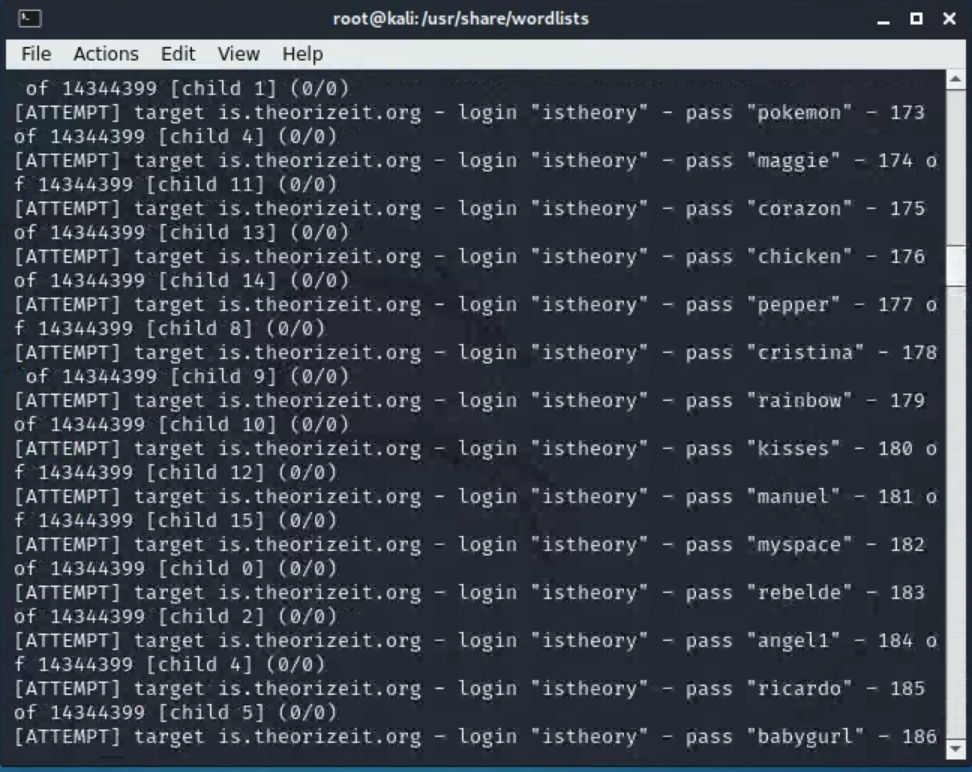




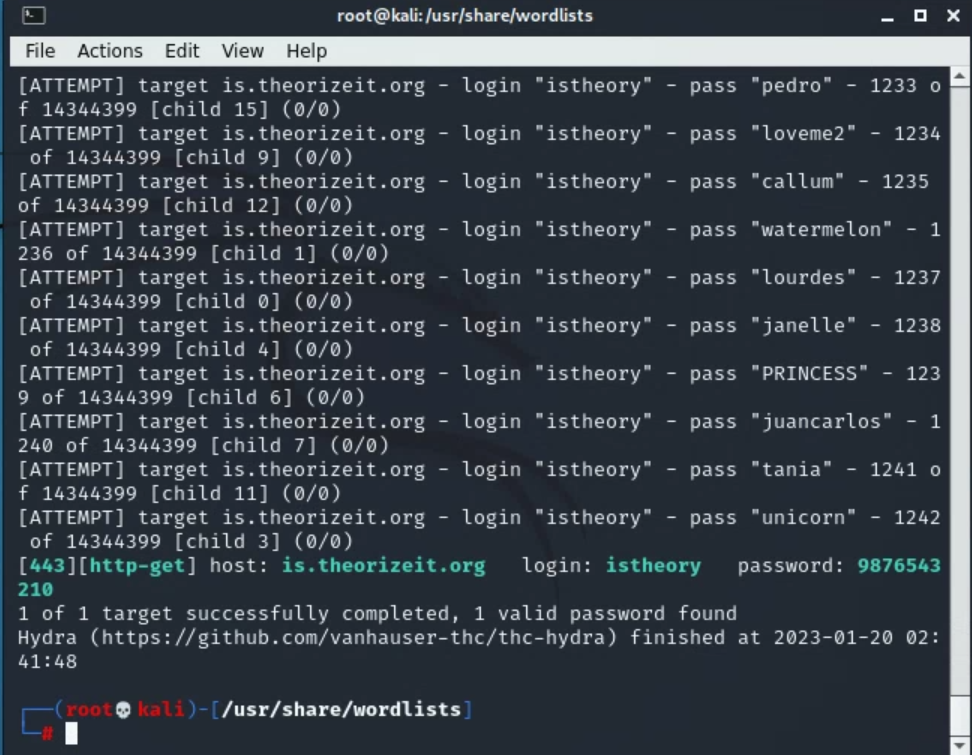
Getting the dependencies for Hydra



Installing Hydra



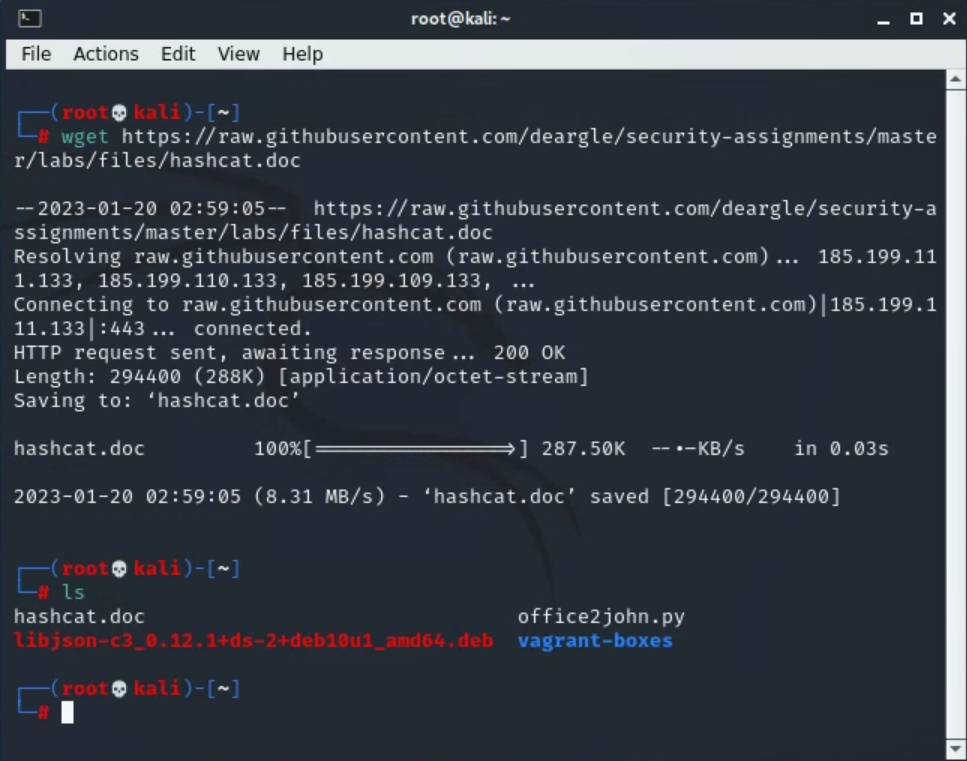
Password Cracked



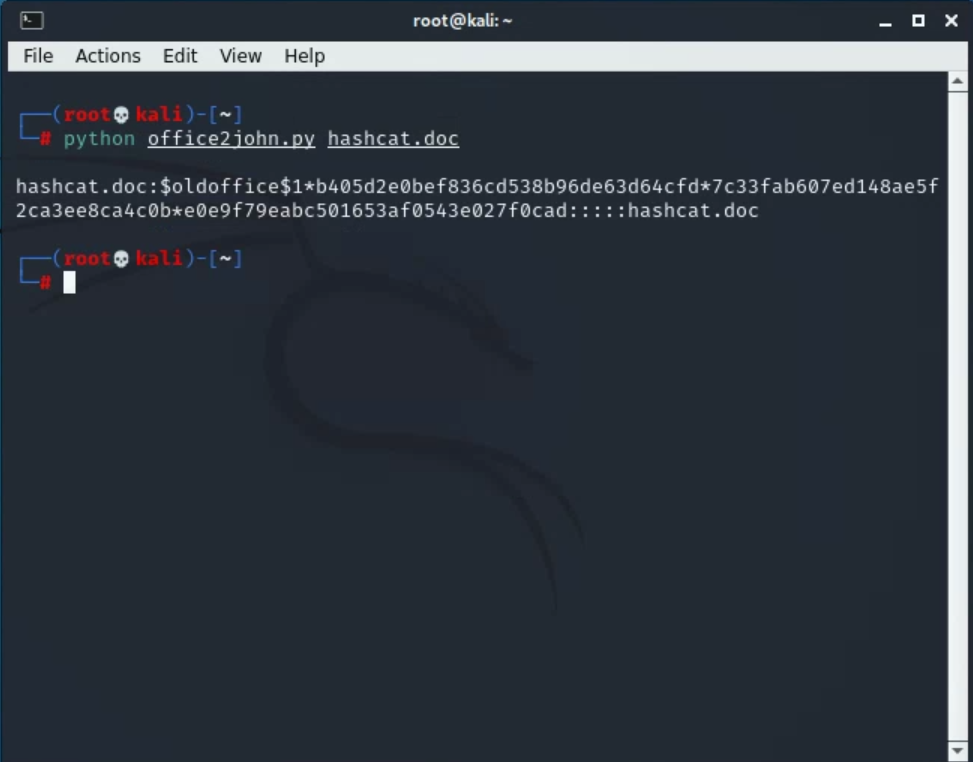
1. **Offline Attacks using Hashcat**



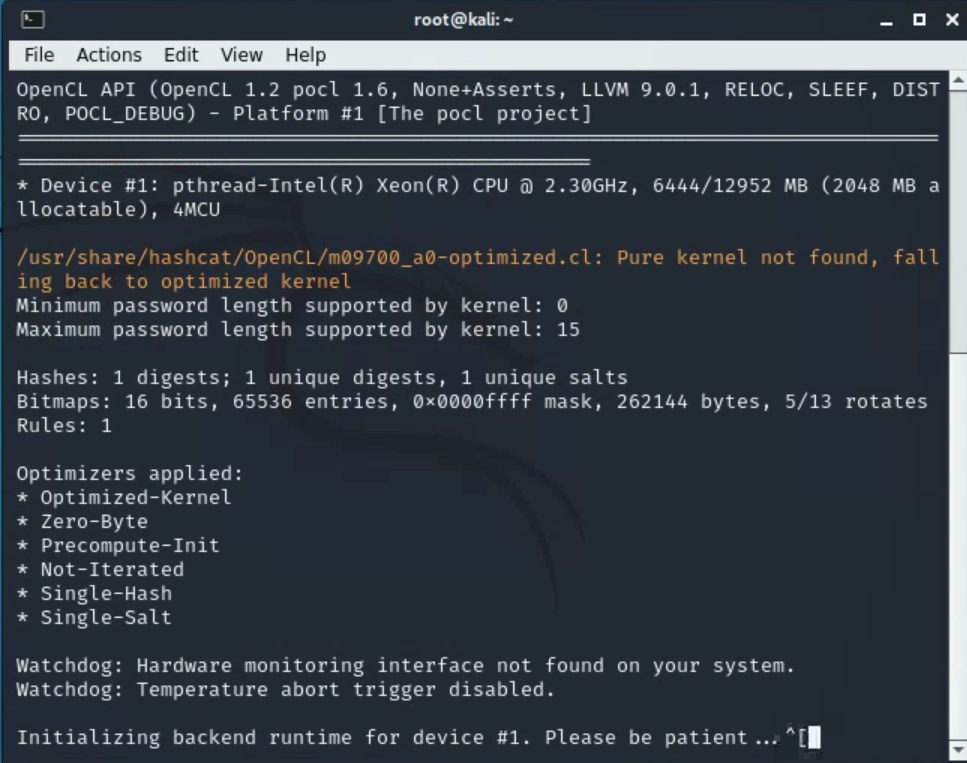
Getting hashcat



Running hashcat



Cracking the hash



Cracked Password : Crash



Password for john.doc

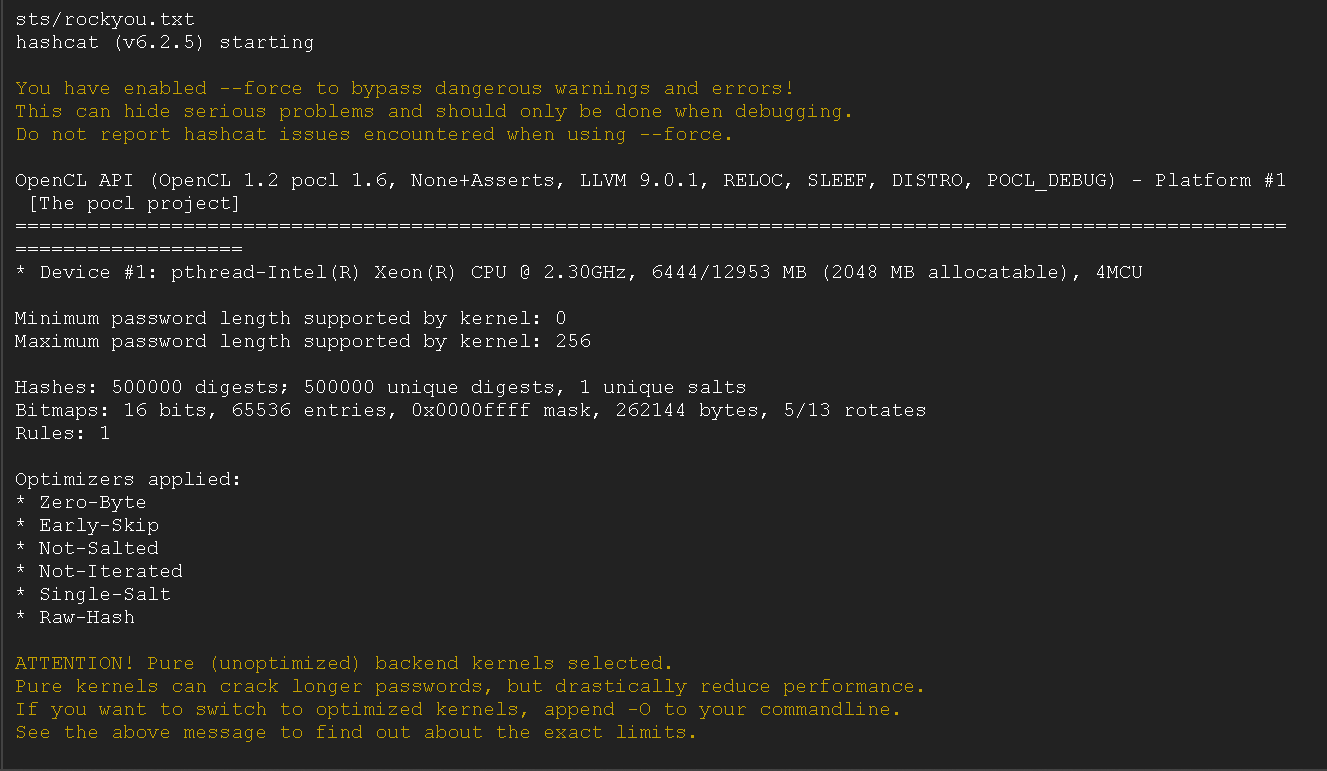


**7. Cracking LinkedIn Hashes Using Hashcat**

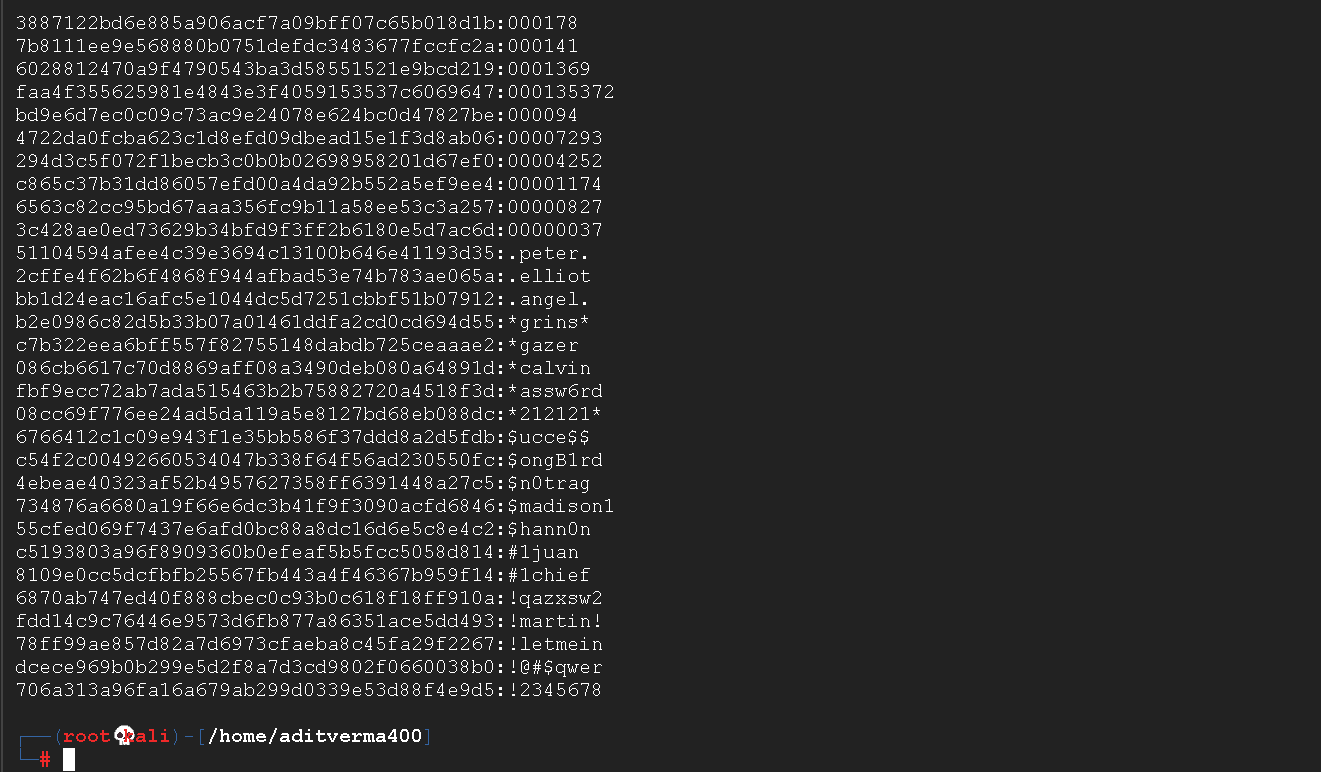
Getting the list of leaked hashes



Running Hashcat



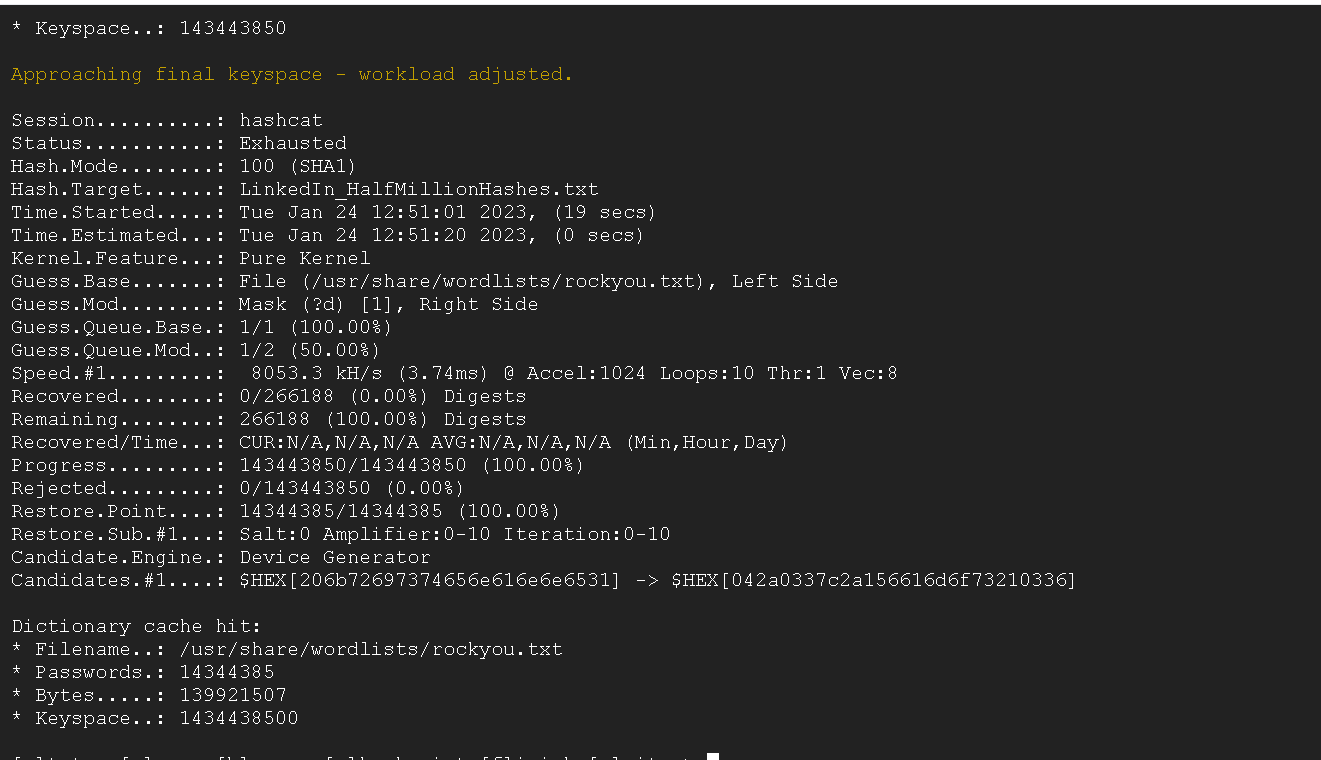
Cracked Passwords



Using hashcat with a -r attribute

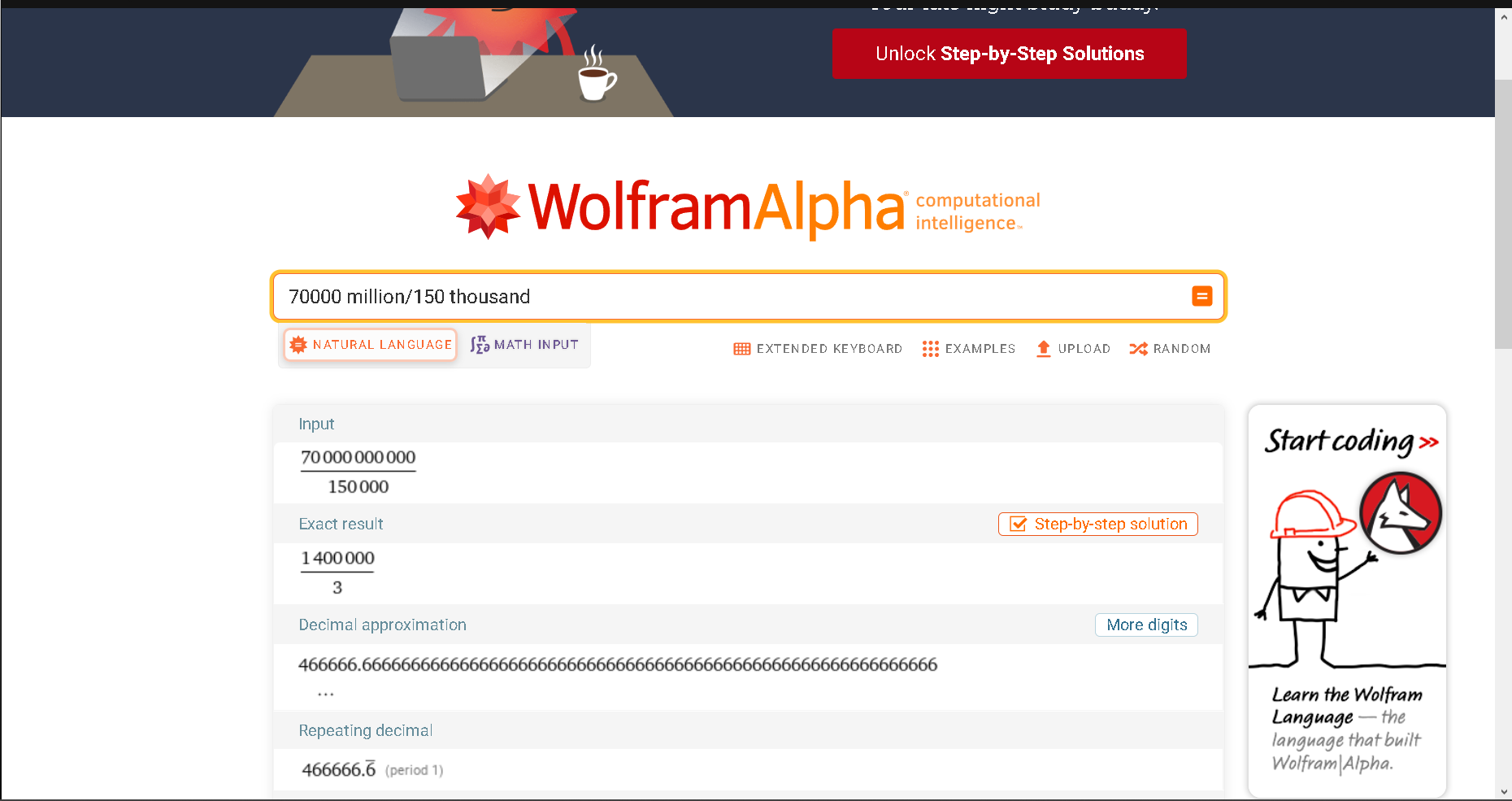


Using hashcat with %d %d

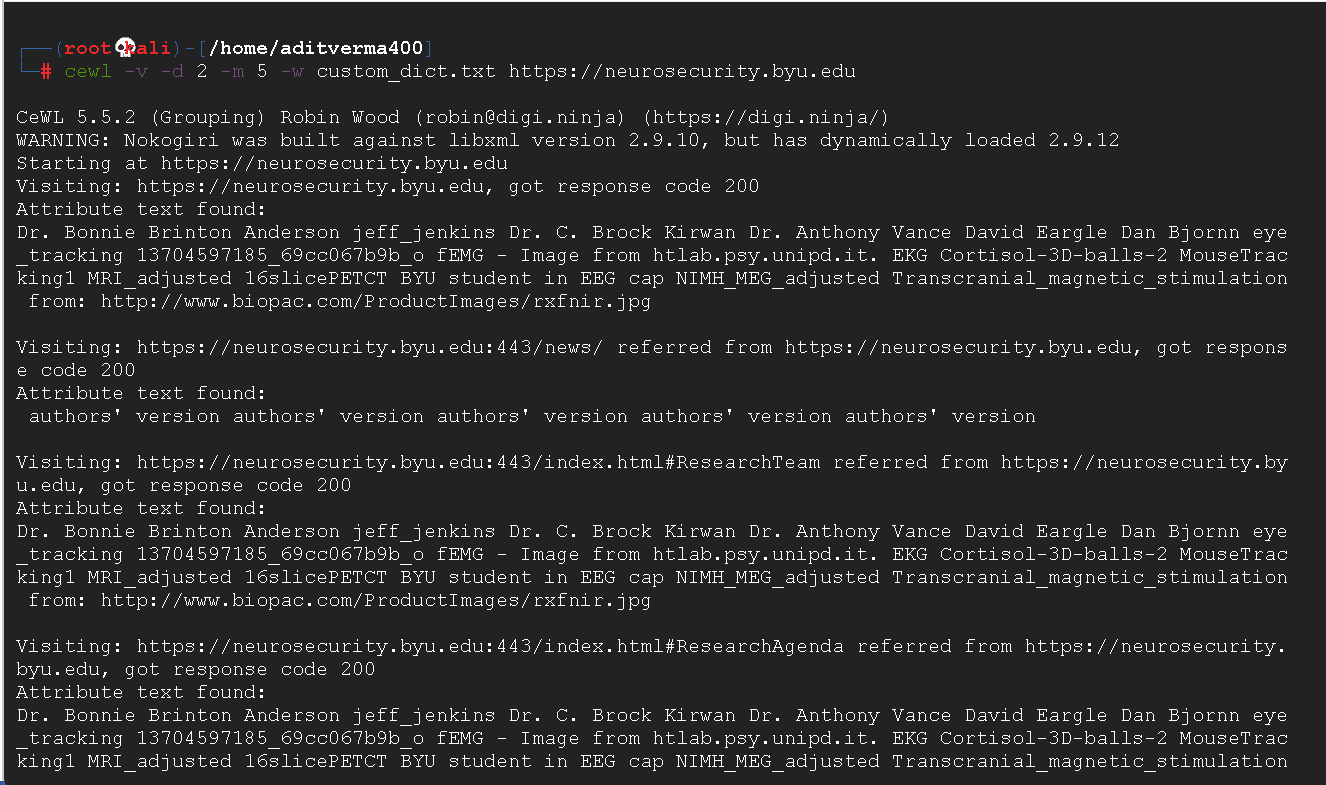


1. **Secure Password Hashing**

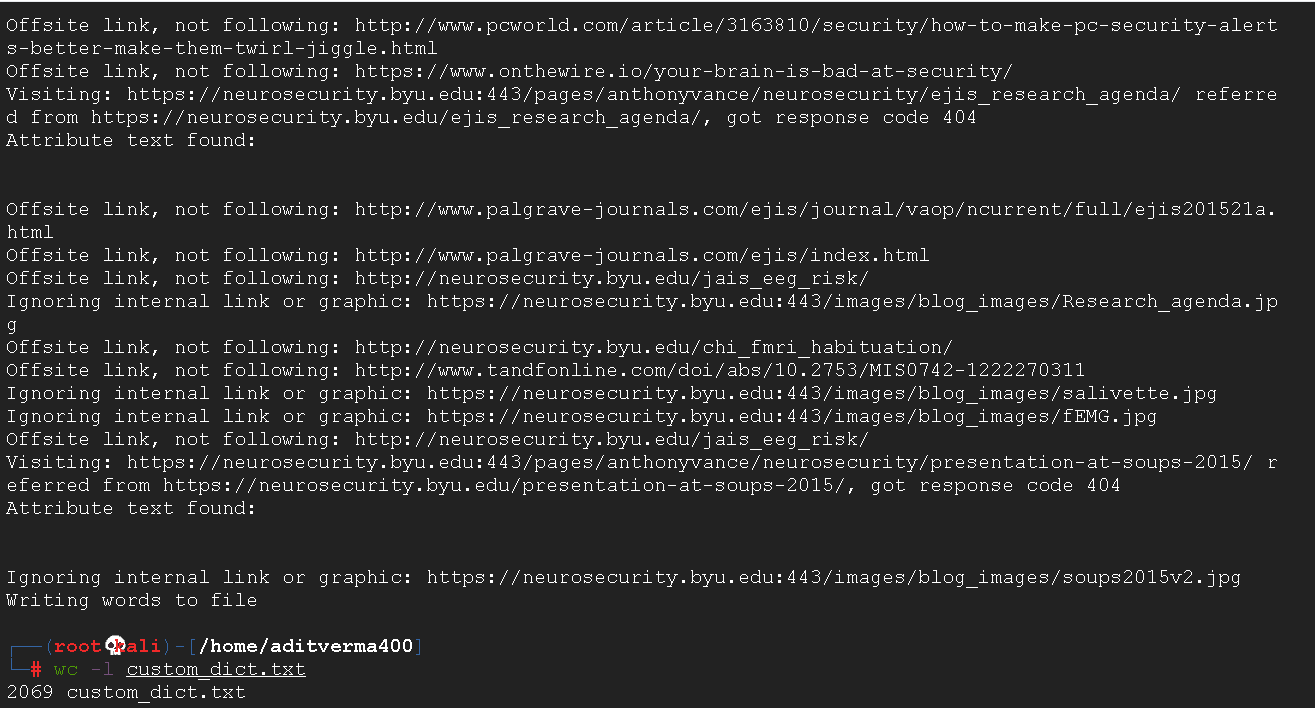
Seeing how powerful a password is



1. **Create a Targeted Wordlist Using CeWL**



Seeing how many terms are there in the file



Looking at the passwords in the file



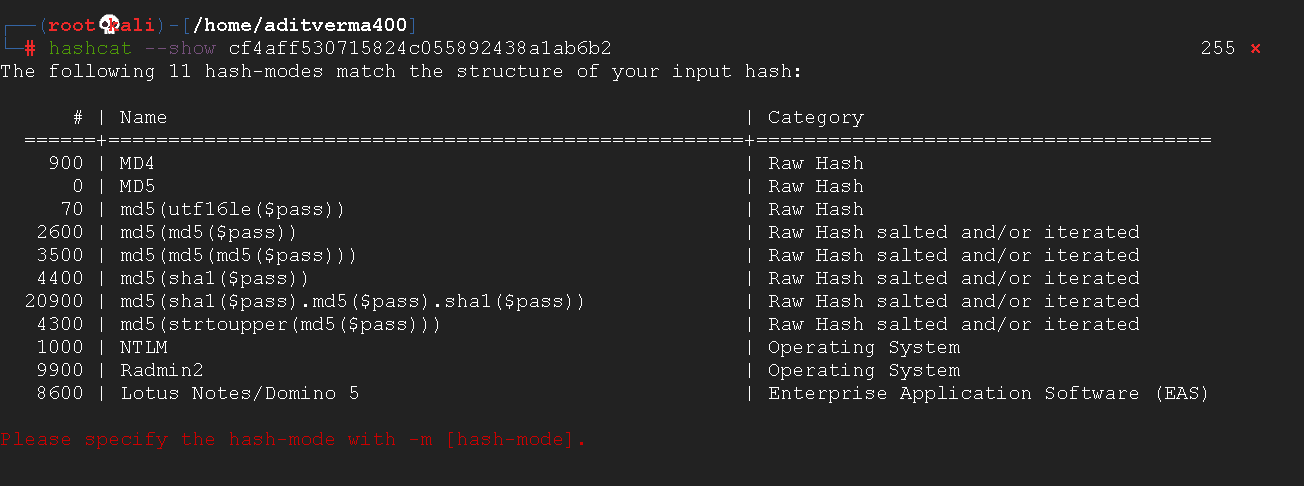
Running hashcat using custom dictionary



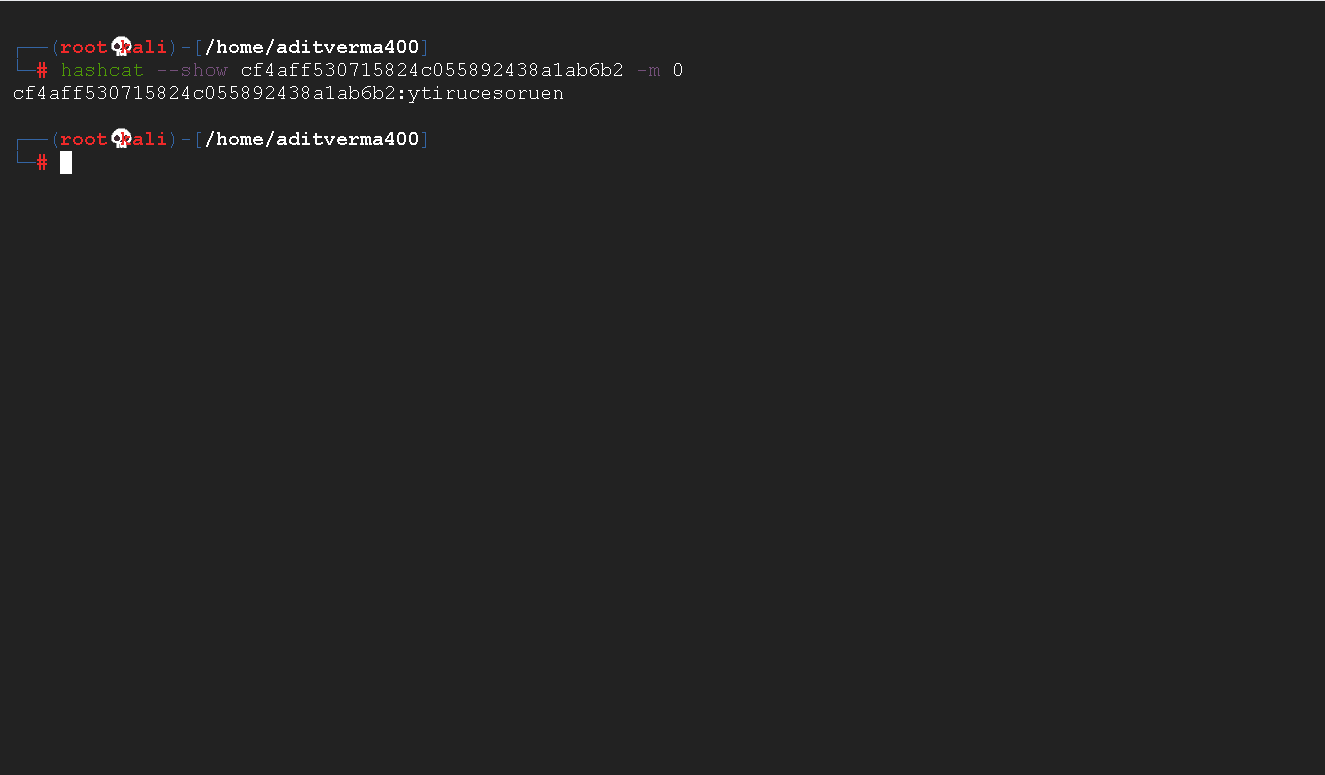
Seeing the entries in the file



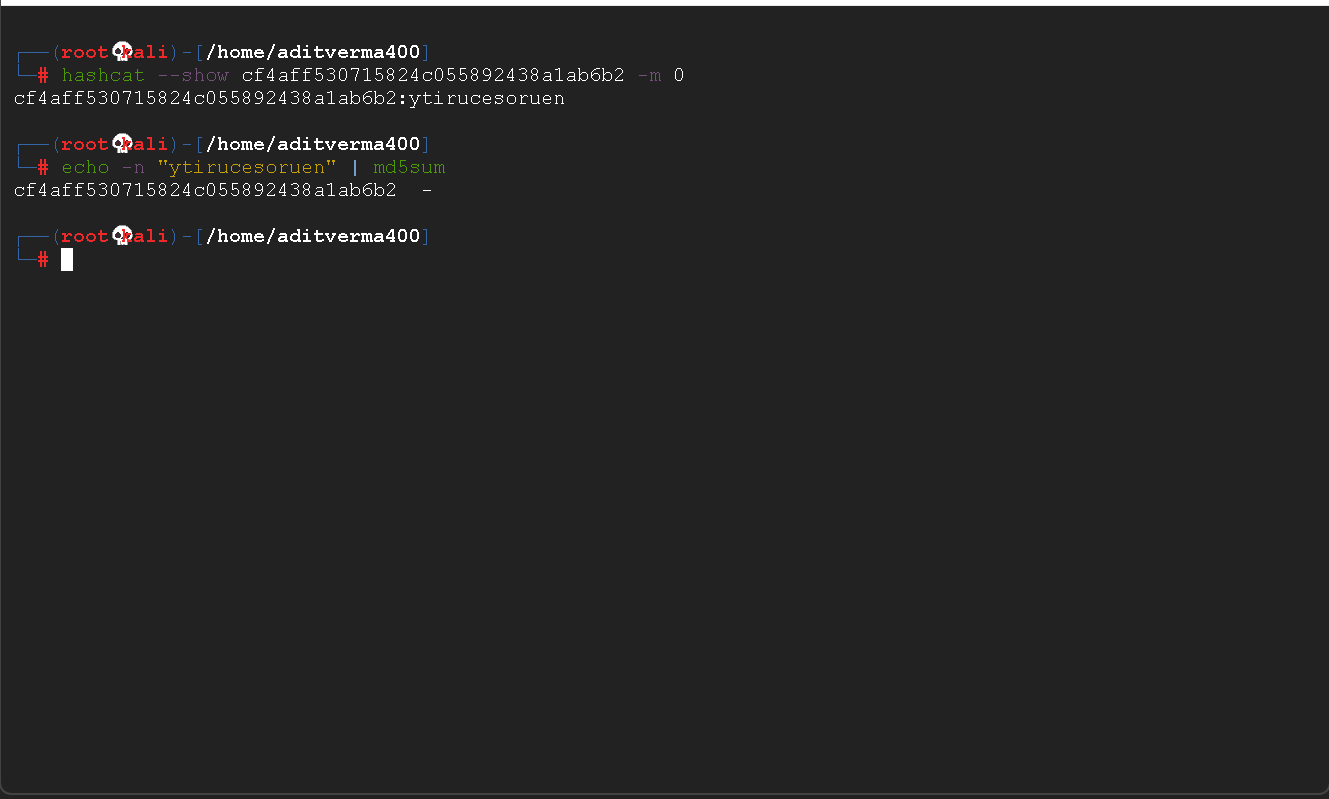




Cracking the hash



Seeing if the hash matches the obtained answers



**Question-Answers –**

**Question 1:**Was one of your accounts breached? If so, which one(s)?

1. Yes my gmail account has been breached in one data breach .

**Question 2:**Which service did you enable 2FA for?

1. I enabled 2fa for gmail.

**Question 3:**Scan the results to find the line beginning with [443][http-get]. What was the password?

1. babydoll

**Question 4:**For the lab submission, you will be asked to look at sample output from a hydra run, and determine how many passwords were tried per second in the sample output.

1. Hydra took 18 sec to crack 1241 passwords. and hence we can calculate that hydra tried 69 passwords per second

**Question 5:**What is the password for hashcat.doc?

1. The password is camp

**Question 6:**What is the password for john.doc?

1. The password is attica

**Question 7:**How many passwords per second can Hashcat running on a Brutalis try on a .doc file (i.e., hashtype “MS Office <= 2003 MD5 + RC4, oldoffice$0, oldoffice$1”)?

1. 1792.9 million hashes per second

**Question 8:**How much faster is Hashcat in cracking .doc MS Office documents (option 9700, “Hashtype: MS Office <= 2003 MD5 + RC4, oldoffice$0, oldoffice$1”) compared to Office 2013 documents (option 9600, “Hashtype: Office 2013”)?

1. For MS Office <= 2003 MD5 + RC4, oldoffice$0, oldoffice$1, the cumulative cracking speed is 1792.9 MH/s For Office 2013, the cumulative cracking speed is 70884 H/s The difference between the two is about 17,928,929,116 or 17.9MH/s

**Question 9:**How does an offline password attack compare with the online hydra attack you attempted earlier?

1. Attacks that are conducted offline are essentially undetectable by security personnel and logging systems.

The compute constraints of our PCs, not the network capacity, are what determine how quickly a breach may be made. As a result, passwords may be cracked relatively quickly. compared to internet assaults, offline attacks

**Question 10:**How many passwords were you able to recover using the Hashcat command above?

1. I recovered 14344385 passwords

**Question 11:**How many total passwords were you able to recover after using this rules based attack in combination with the earlier straight attack?

1. I recovered 89190 passwords

**Question 12**: How many total passwords were you able to recover after using this hybrid attack in combination with the earlier straight and rules-based attacks?

1. I was able to recover 0 passwords

**Question 13:**How much slower is Hashcat in cracking Bcrypt hashes compared to SHA1 hashes?

1. Hashcat cracks 6.87709 x 107 kH/s more SHA passwords than Bcrypt in the same time

**Question 14:**Imagine that Bcrypt is set to a work cost factor of 12. How many hashing rounds will Bcrypt go through to compute the final hash?

1. It would take Brypt 2 12 = 4096 rounds

**Question 15:**An attacker knows that a user generated their password using 8 random lowercase letters exclusively (so character space of 26, length of 8). On average, an attacker needs to try only half of all possible passwords in order to brute force the password. The attacker has access to a Brutalis. How long would it take to crack the password hash if SHA1 had been used? How long with bcrypt using the benchmarks shown for a Brutalis?  
**A)** The cracking speed for SHA1 is 68771.0MH/s.

Password space has a total of 268 potential passwords, or 208827064576 passwords.

For a crack, he must unhash half of the aforementioned amount, i.e., 104413532288.

The time it will take to break all 104413532288 passwords is 104413532288/(68771.0 MH/s) = 1.5 seconds.

The cracking speed for bcrypt is 105.7 kH/s.

Password space has a total of 268 potential passwords, or 208827064576 passwords.

He needs to unhash half of the aforesaid amount, or 104413532288, for a crack.

It will take 104413532288/(105.7 kH/s) = 987829 seconds or 11.4 days to break all 104413532288 passwords.

**Question 16:**What is the plaintext of the hash?

1. The plaintext is ytirucesoruen