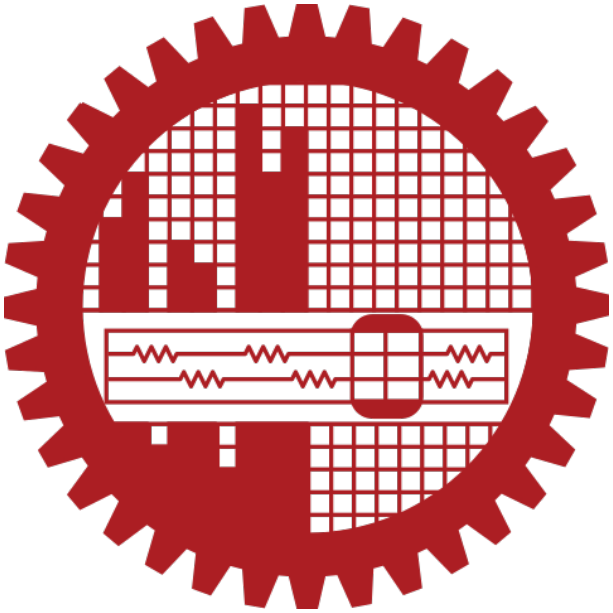

Computer Security - CSE 406

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

DICTIONARY ATTACK

Made by:
Ahnaf Faisal
ID: 1505005

Contents

1 Definition

A dictionary attack is a technique or method used to breach the computer security of a password-protected machine or server. A dictionary attack attempts to defeat an authentication mechanism by systematically entering each word in a dictionary as a password or trying to determine the decryption key of an encrypted message or document.

Dictionary attacks are often successful because many users and businesses use ordinary words as passwords. These ordinary words are easily found in a dictionary, such as an English dictionary.

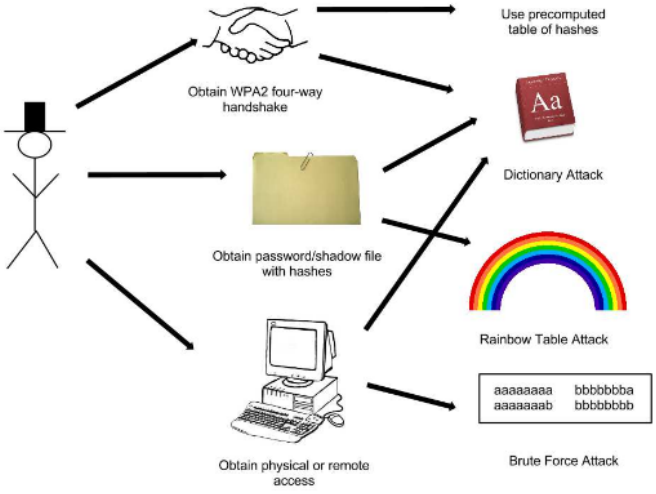

Figure 1: Password Cracking

2 My Implementaton

I have tried to show case 3 examples of dictionary attack. One of them is online based in seed ubuntu xsslabelgg site. The second one is a offline based where the attacker will have the hashed password file of victim.The other online based is where I build my own server and have a defence mechanism.

3 Seed Apache Server Attack Implementation

By observing the http packets through wireshark and http header, I saw the seed elgg site provides a cookie when a get request to their site is sent. The returned page also contains elgg token and elgg timestamp which then can be used to invoke the login post method.If the credentials are correct, it will reply with a new cookie. Using that cookie, one can get the desired log in page.
In 3 the desired password is in 2nd position,so login is no problem and we get 3 page.

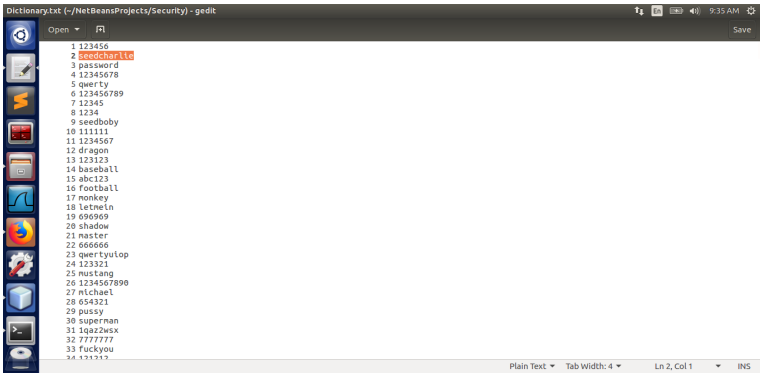

Figure 2: Dictionary File

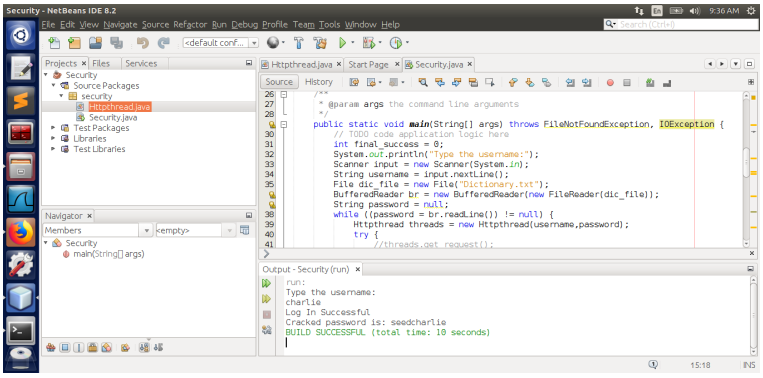

Figure 3: Input Line

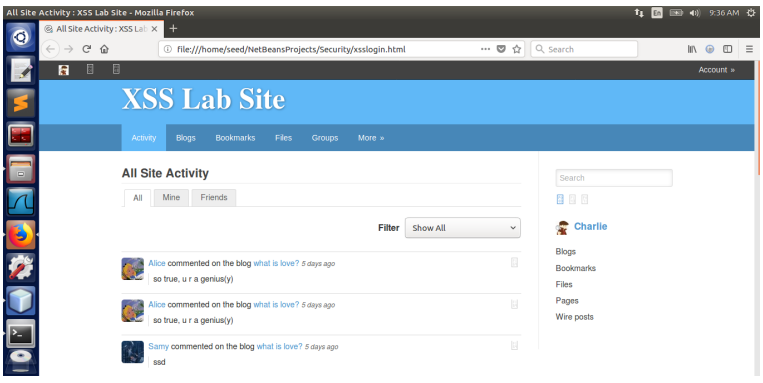

Figure 4: Result site

But seed elgg site has security mechanism which locks the account after some failure attempts.So if the password is in far position the attack will fail like in 3.

Figure 5: Failure condition

4 Offline File Password Cracking

In this case, I deal with a password file containing usernames,hashed passwords and sometimes their salts. Hash is done in two ways, SHA-1 hash and reverse string sha hashing.

Firstly all the usernames and hashed passwords are put in a hashmap. Again, from the dictionary

```
andrew 0 7207aa5e5e68188241a72b3fd9b12391585cad21
joe 0 65640c6577c9c72497525e656127b5bd1deb6f85
eve 0 61424ee758ec5e0d0ffe6a2ce151bf9d927c3ad7
bob 0 843b961da8707a9314aa3b7bb950a7003e49a94c
guy 0 eb6dc8cf797e6aeec2f2695883c0cf93cc765537
alice 0 eb756abf97413f28b2e36f1de57e17b31129aa46
mary 0 932eeb1076c85e522f02e15441fa371e3fd000ac
adam 0 7d27662bb31cb629178e929287993c01bf7c42ac
nick 1 a9edd3db 93bbd7dab6e365a5a840584d9849cbd55fbbf469
john 1 2afd4f21 511c896b5bcf313140d513100966a5ccec90c714
ahnaf 0 d0be2dc421be4fcd0172e5afceea3970e2f3d940
mahim 1 3452345a ea7a39ddd61217af562073ec9849dcf7a723d2a0
```

Figure 6: Password File

all the hashes are precomputed although in cases of salt it does not serve any purpose.

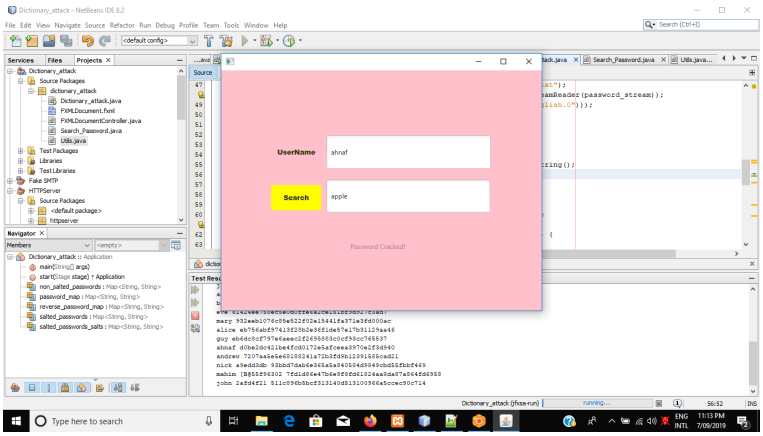

Figure 7: nonsalted password login

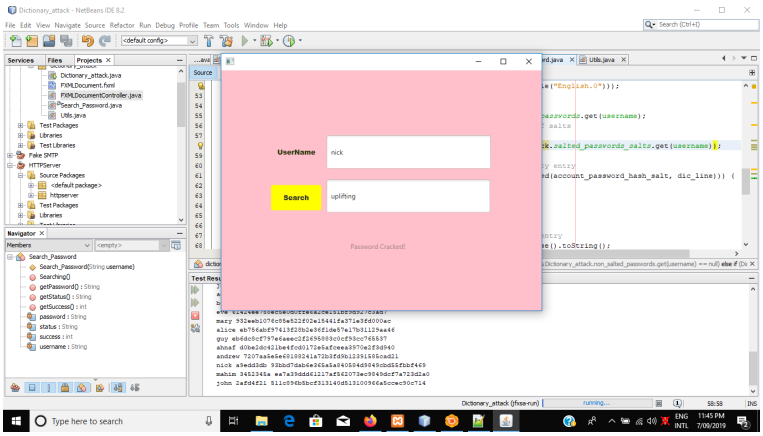

Figure 8: salted password login

4.1 Defence Mechanism

If the salts are not in the password file or saved elsewhere there is no way the attacker can crack the correct password.

5 My Victim Server

I implemented a server which responds to get and post requests made on localhost port no 6780.Responding to get requests it responds with html page.

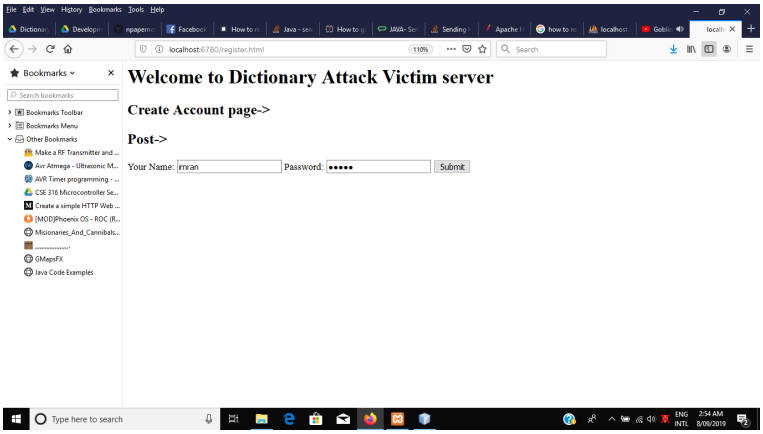

Figure 9: Register html page

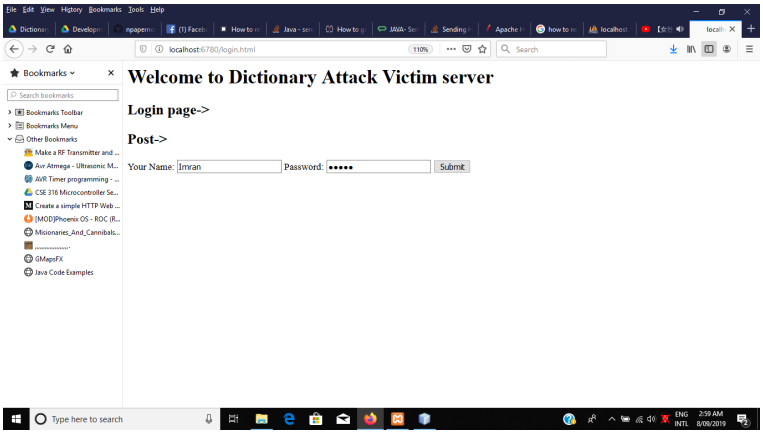

Figure 10: Login html page

When a post request is received along with username and password field, it computes the hash of received password and compares it with the stored hashed password of that user. If it matches then it replies with 5 page.

If credentials dont match or the username doesnot exist,then it replies with 5 page.

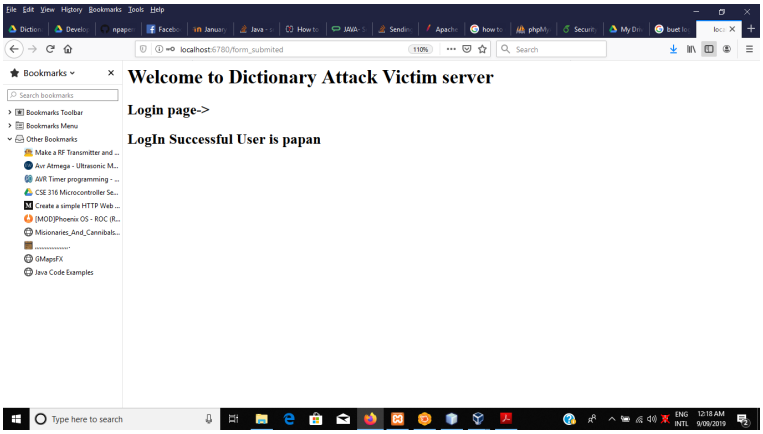

Figure 11: Success login page

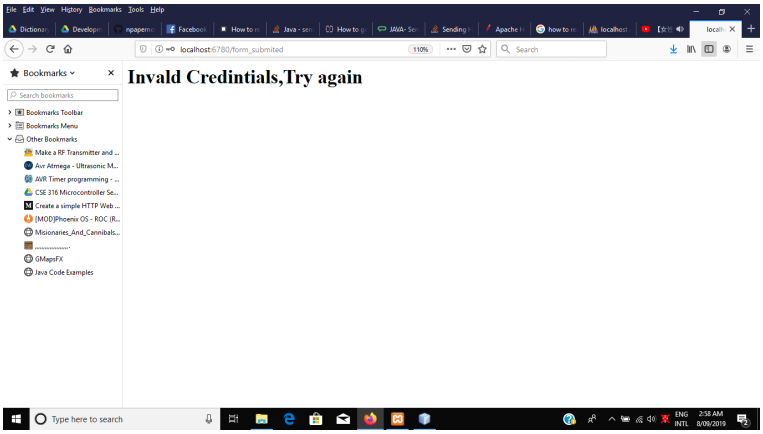

Figure 12: Invalid login

So the attacker tool sends post request containing username and predicted password from dictionary file and retrieves the response page. If response page contains login successful that means the password was correct and our job is done.Otherwise it will continue sending dictionary words.

5.1 Defence Mechanism

My server has a defence mechanism flag which when activated keeps track of consecutive unsuccesful logins. If it exceeds the limit number then the account will be locked and will repond with account locked page.

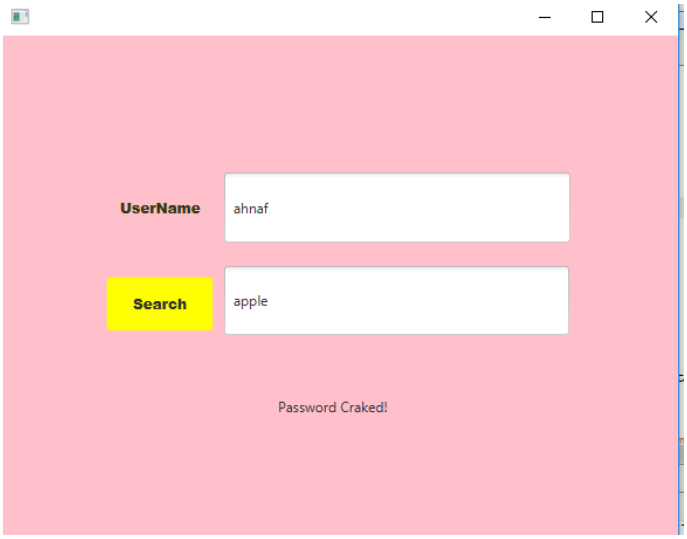

Figure 13: Login from Attack tool

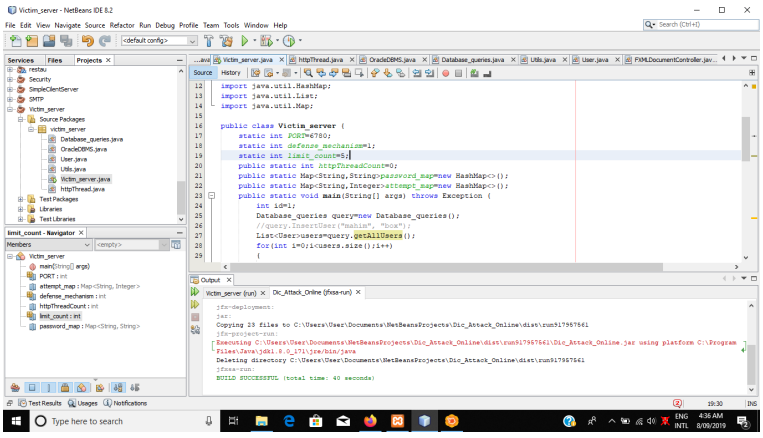

Figure 14: Code Portion Defence flag

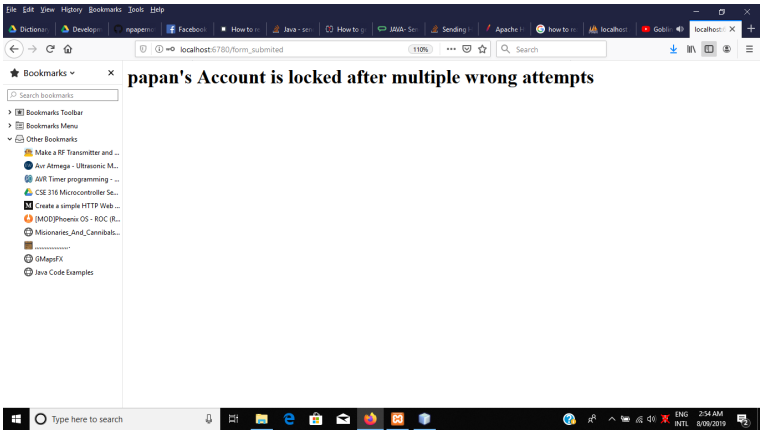

Figure 15: Locked Account

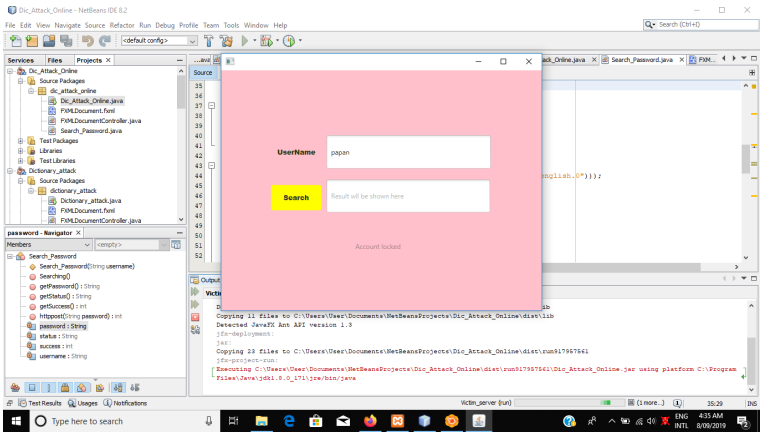

Figure 16: Locked Account

6 Conclusion

So in my three attacks, one I used seed ubuntu elgg site,other with offline password and last one with my own made server with protection mechanism.Due to hardware limitations I stick to reading from one dictionary file because opening large dictionary files at once not much feasible and time efficient in my machine.In powerful computers the process can be speeed up multiple threads or even using multiple computers at a time.