COMP522: Privacy and Security

http://cgi.csc.liv.ac.uk/~alexei/COMP522/index.html

University of Liverpool

Lecturer: Alexei Lisitsa

Lab 1 Practical Attacks on Passwords

LAB #1.1 –Hash table attack

Given a hash of the password, can you recover a password?

0- Create a hash to any password that you want to attack, you can use www.sha1-online.com for that (or any other). For example, the SHA1 hash for password MyPassword is daa1f31819ed4928fd00e986e6bda6dab6b177dc

1- Copy the hash and go to any public sha1 hash table website and try to get equivalent text to it. (you can go to https://sha1.web-max.ca/)

2- Can you do hash table attack for the following password (sha1 hash) by using the same website.

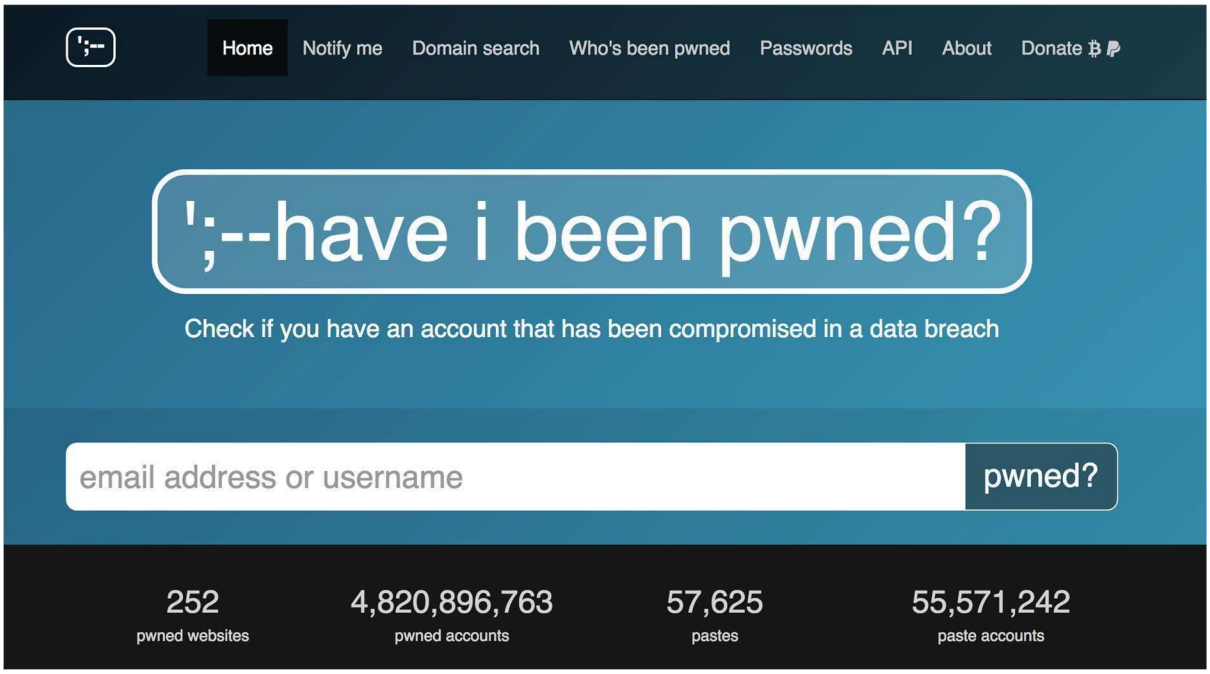
N	Password	Yes I can / No I can not
1	P@$$W0rD	
2	Thisismypassword	
3	VeryLongP@$$W0rD	

3- What is a shortest password you can find for which the above hash table attack is unsuccessful?

LAB #1.2 – Have My account password leaked to attackers

1- Open https://haveibeenpwned.com/

2- Provide your email and check if your account password has been leaked before by the attacker. If you, you have to change your password.



LAB #2.4 – How long to offline brute-force password

Note: - Don't Enter your real password - The time it will take depends on processing speed

1- Open https://www.security.org/how-secure-is-my-password/ and https://password.kaspersky.com/

2- Try the following passwords in the table and check the time needed to brute-force them and reported strength

3- Can you propose a password which you would easily remember and which would have estimated 1 Day to crack it (by either services)?

Password	Time on security.org/how-secure-is-my-password	Strength on Kaspersky password checker
P@S$W0rD		
thisismypassword		
VeryLongP@$$W0rD		
%O^t#2Fv0JUjVdRV2RW%		
