Exercise: Sensitive data exposure; Solutions

Solution

Read your passwords

Exercise 1. In this exercise, we see why crypting data, without secure storage of the key is not sufficient. You first need to download LaZagne

```
$ git clone https://github.com/AlessandroZ/LaZagne.git
$ cd laZagne
$ pip3 install -r requirements.txt
$ cd Linux/
$ python3 laZagne.py browsers -firefox

------------------- Firefox passwords -----------------

[+] Password found !!!
URL: https://www.amazon.fr
Login: test_bfh_amazon@benoist.ch
Password: 4bTYXj7dfdfdfdf


[+] Password found !!!
URL: http://localhost
Login: emmanuel
Password: emmanuel

[+] Password found !!!
URL: https://www.benoist.ch
Login: emmanuel
Password: TestPassword


[+] 3 passwords have been found.
For more information launch it again with the -v option

elapsed time = 0.26378583908081055
```

Unsalted passwords

Exercise 2. We use CrackStation to hack unsalted sha1 hashes. Just copy and paste the values inside the input field.

Username	Hashed Pwd	Password	Status
bie1	8da4d36229d9b0eb24a9e7c875151a66e5a9eb19	toto72	Found
doj1	1f71e0f4ac9b47cd93bf269e4017abaab9d3bd63	bonjour	Found
due1	59d9a6df06b9f610f7db8e036896ed03662d168f	Hallo	Found
arb1	8cb2237d0679ca88db6464eac60da96345513964	12345	Found
frc1	e8dd41e392fc88d355adc5ce95805975c7baffd6	Kj56I-0	Not found
hnr1	ba1630afffe80fe0e5fcf353cc9dc245ef2683a9	gju98	Not found

Related Pages

Home

Slides

Exemples

Exercices

Resources

Contact

Prof. Dr. Emmanuel Benoist
Berner Fachhochschule - TI
Quellgasse 21
CH-2501 Biel/Bienne
Switzerland
Mail: emmanuel.benoist (at) bfh.ch

Social Networks

Follow me on
Linkedin, Scholar & Research gate

http://www.ti.bfh.ch/

knr1	8be3c943b1609fffbfc51aad666d0a04adf83c9d	Password	Found
ert1	db8ac1c259eb89d4a131b253bacfca5f319d54f2	HelloWorld	Found
sdf2	7e6dfeb48afce444b8be7b274b7e0869bd7c9c86	MorgenZäme	Not found
yxc3	5a7f6ec9cdb4dc7035dc03c36e8d48f463cf339c	GoodMorning	Found
ztr1	fb4d8deebe0cd2ae130336c889897f72234586eb	Thisismypassword	Found
lkj1	06da63dbb1896fb91bfac21d3ede356aa69e0db6	Bonjourlemonde	Not found
opi2	1f71e0f4ac9b47cd93bf269e4017abaab9d3bd63	bonjour	Found
mnb3	048302433b4d42b6fc68f92ffca414a9a976dd46	MotDePasse	Found
rut1	1bba086040e9071efd98e303ea4758b1d91f05b5	Password2015	Not found
edc2	789ba01887bc4bf6495465a2e007c641259d013f	bonjour2015	Not found
rfv3	b518312d4755b54f8155e0f7c26b12eca1474287	MotDePasse2015	Not found
tgb1	daa1f31819ed4928fd00e986e6bda6dab6b177dc	MyPassword	Found

Conclusion: even without any effort we could hack half of the passwords. Hash without salting is useless for passwords. Even long passwords could be descovered provided they are in lists of found passwords.

Hashcat for salted passwords

Exercise 3. Suppose we have a file rockyou.txt containing a list of possible passwords. You will have to store such a list if you want to work in that business. (it could be initialized with the list of crackstation for instance).
We use the mode sha1(hash:salt) with number 120, so we need to write our inputs on the form hash:salt (our salt is username plus ';'). This produces the following file: hashWithSalt.txt
First attempt: try with all passwords in the list:

```
hashcat --force -m 120 hashWithSalt.txt rockyou.txt
```

Brute force: Writes out the output in the file result.txt (-o is for output)

```
hashcat --force -m 120 -a 3 -n 5 --custom-charset1=?l?u hashWithSalt.txt ?1?1?1?1?1 -o result.txt
```

It tests all passwords with length between 4 and 6. For length larger than 8, you need a dedicated machine (with a great GPU). Or better, you use a list + some rules.
Hacking passwords requires a lot of testing and sometimes works.

Conclusion

- Passwords shorter than or equal to 8 are easy to bruteforce
- Passwords that are in a dictionary are easy to be found
- Passwords based on two concatenated words are easy to be found (even if much larger than 8)
- Here are some of the first rules used by attackers: First letter is capital, two digits in the end, all easy replacement rules (E->3, O->0, l->1, ...). They apply this to allready found passwords or to dictionaries.

BACK TO TOP