# The Anonymous attack on HBGary

Jarib Rahman
March 19th, 2012

# Background

December 2010: Anonymous takes down corporate websites of Bank of America, MasterCard, Visa, Paypal and others. This is retaliation for these companies deciding to freeze donations/not provide services to Wikileaks.

HBGary Inc. is a security firm that provides security software and services, including malware detection and analysis,  secure networking, pentesting, etc.

February 5, 2011: Then CEO of HBGary Federal, Aaron Barr, tells Financial Times that he managed to uncover some information regarding Anonymous. He claims to have done this using fake identities on social networking sites.

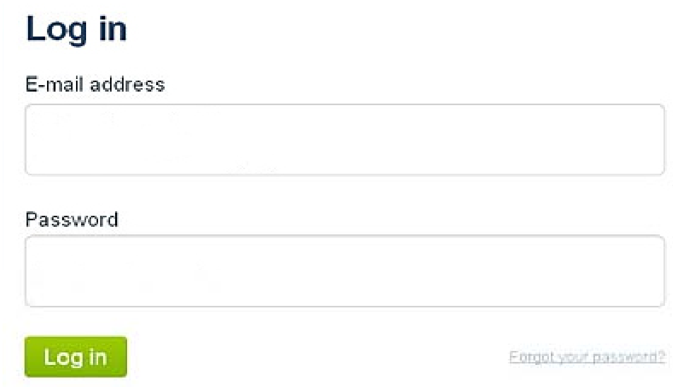
February 5-6, 2011: In retaliation, Anonymous breaks into HBGary servers, destroys its data, publishes its email, hacks into Aaron Barr's twitter account and posts his personal information, publishes his emails, takes down a website owned by HBGary owner Greg Hoglund – rootkit.com, publishes its user registration database.

# The Attack

1. SQL Injection to obtain user database.

# Basic SQL Injection

Forms which ask for information are turned into sql queries:



```
SELECT * FROM users WHERE name =
'$userName' and password =
'$password';
```

Badly written code to parse sql queries can be exploited to extract information from the database. Let's say the following code is not checked for escape characters:

```
SELECT * FROM users WHERE name = 'admin' -- and password = ' ';
```

This query can be generated with an input of `admin'--` in the username field, with the password blank.

# Basic SQL Injection (Continued)

```
SELECT * FROM users WHERE name = 'admin' -- and password = ' ';
```

`--` is a comment, hence after 'admin', rest of query is commented out. Thus, there are no password checks. If the code does not check for characters such as `--` then there will be no password check.

Another example:

```
SELECT * FROM users WHERE name = 'anything' or '1'='1';
```

If the input is `anything' or '1'='1`, the last ' makes the query evaluate to a boolean statement with OR in the middle, and `'1'='1'` as the second part of the statement. Always evaluates to TRUE.

Queries can be generated as such by specific inputs, or writing specific URLs in the case of forms using the POST method.

# The Attack

**1. SQL Injection to obtain user database.**

Specific query that was used to break into database:

```
http://www.hbgaryfederal.com/pages.php?pageNav=2&page=27
```

Usernames, email addresses and password hashes were obtained.

# The Attack

**2. Rainbow tables to crack password hashes.**

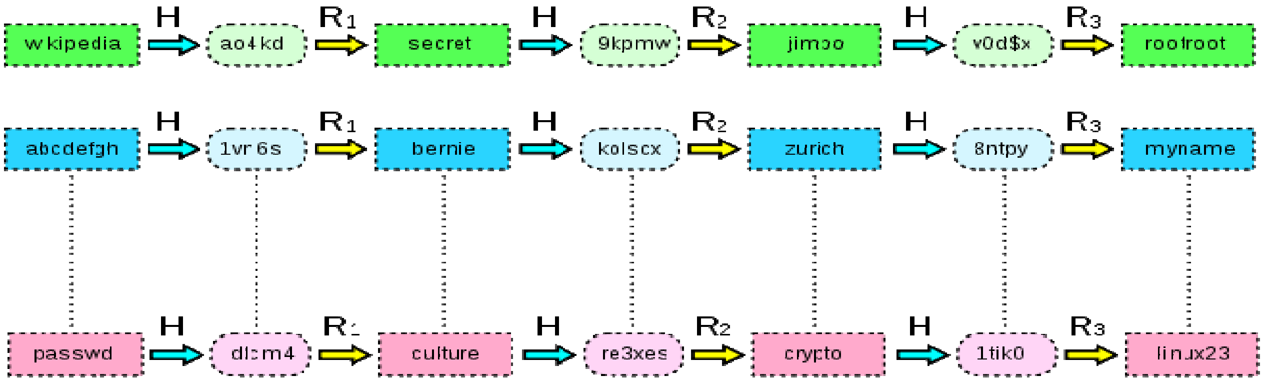
# Rainbow Tables

Used to crack password hashes to obtain password.

Cryptographic hashes for common passwords are precomputed and stored in a table.

Hashes of all possible passwords must be computed. If set of all passwords is S, the size of this table will be O(|S|n), where n is the number of bits in the hash.

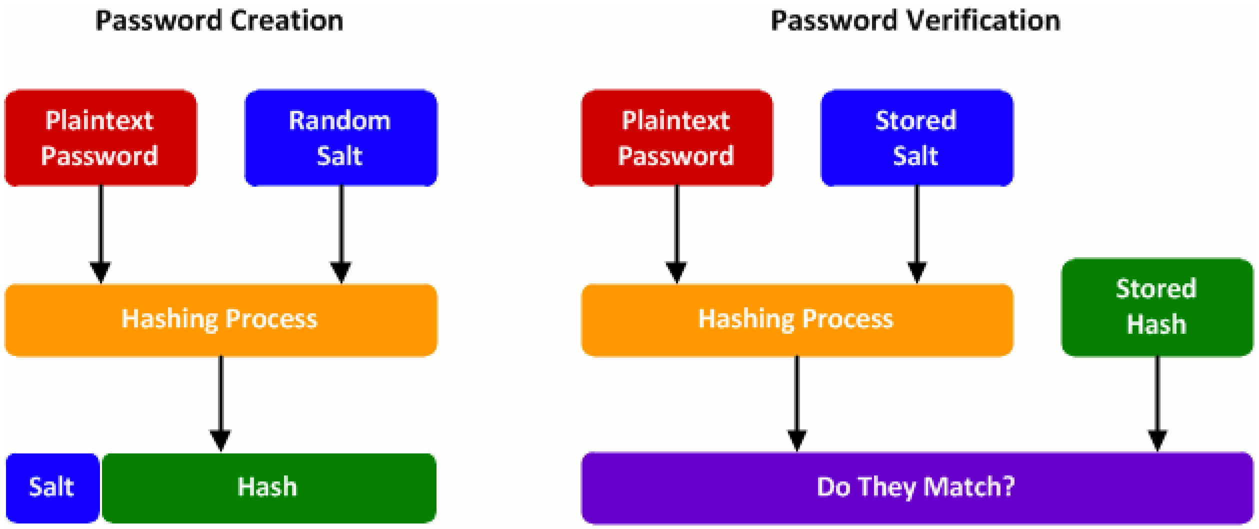
This requires a lot of space, but reduction functions can be used to reduce storage significantly.



# Salting

Add a bit of 'salt' to password before generating its cryptographic hash.

The salt is usually a random value. This ensures that the same password used by different people will result in different hashes for each person.



# Iterative Hashing

Output of hash function is also hashed with the hash function, and this is repeated about a thousand times.

Simple example:

```
key = hash(password + salt)
for 1 to 65536 do
  key = hash(key + password + salt)
```

# The Attack

**2. Rainbow tables to crack password hashes.**

Salting and Iterative Hashing were not used in HBGary database.

It used MD5.

CEO Aaron Barr and COO Ted Vera used very simple passwords: 6 lowercase letters and 2 numbers.

# The Attack

**3. Exploit password reuse.**

Aaron Barr and Ted Vera used same passwords for email, twitter, etc.

Ted Vera's password was used to ssh into HBGary machine. Ssh did not use keys, but passwords.

Ted was only a regular user. In order to escalate his privilege level to that of a superuser, a known exploit involving system libraries was used, for which patch came out in October 2010.

# References

[1] http://abcnews.go.com/Technology/wikileaks-anonymous-cyber-attacks/story?id=12355960&page=2#.T2WtWtU1RU0

[2] http://www.ft.com/intl/cms/s/0/87dc140e-3099-11e0-9de3-00144feabdc0.html#axzz1pShFW6fm

[3] http://www.v3.co.uk/v3-uk/news/2030767/researcher-claims-infiltrated-anonymous-command

[4] http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars/

[5] http://en.wikipedia.org/wiki/Rainbow_table

[6] http://kestas.kuliukas.com/RainbowTables/

[7] http://www.cisco.com/web/about/security/intelligence/sql_injection.html

[8] http://www.unixwiz.net/techtips/sql-injection.html