Secure Communications

Hashing Investigation

Mark Cummins, ITB

You've been asked by the Garda to assist in helping to retrieve some hashed passwords. They have managed to get a dump of one of the database tables, however they still need the original passwords and have been unable to crack them themselves and have called in your help.The issue seems to be that the database is only storing the password hashes, and so far their attempts to brute force the passwords have failed.

They have tried their standard rainbow tables without success and suspect that the passwords may have been salted. A brief analysis of the hashes supports this belief and indicates that all the passwords have been hashed with the same salt.**Can you help the Garda and crack any of the salted hashed passwords?**

Some potentially useful information from the Garda case files:

- The password policy file was changed in May 2010, passwords created after this date are alphanumeric 5-7 characters in length. Passwords created before these dates are believed to have consisted of only digits and 5-7 characters in length.
- It's believed that all passwords have used the same salt, and that the value is somewhere in our data.
- The database dump was from MySQL database
- The site's domain name is www.exploringsecurity.com
- Some of the captured JavaScript code from the site, reveals the salt format as `CommonHash($salt,$pass)`
- Retrieve as much information as you can from the dump below for the Garda

Join_date	Username	Password	Role	Last_accessed	Pass_modified
2009-06-07	Sparky	2834da08d58330d8dafbb2ac1c0f85f6b3b135ef	Admin	2011-09-12	2011-05-09
2010-06-03	Mark123	92e54f10103a3c511853c7098c04141f114719c1	user	2011-01-20	2010-06-03
2009-09-02	superman	437fbc6892b38db6ac5bdbe2eab3f7bc924527d9	user	2011-09-01	2011-01-01
2010-01-11	security	fafa4483874ec051989d53e1e432ba3a6c6b9143	user	2011-10-07	2010-01-11
2009-12-03	Tomtom	06f6fe0f73c6e197ee43eff4e5f7d10fb9e438b2	user	2011-10-03	2009-12-03
2010-04-11	JillC	f44f3b09df53c1c11273def13cacd8922a86d48c	user	2011-04-19	2010-12-20

You should submit a detailed report outlining each step of your investigation including dead-ends and reasoning for each step along the way. Your report should be <1000 words. You should reference any materials, resources used separately.