**PASSWORDS - UNIVERSAL PROBLEM?**

I have a hobby of collecting passwords from all those friendly people trying to logon to my ssh server (see here and here) and it provides me lots of fun. But recent events have prompted me to wonder if the passwords I was seeing are representative of what is actually useful? So I decided to see if I could find out. There first stop is the SkullSecurity site (see here) where Ron Bowes has been kind enough to host some of the leaked passwords from some big events, lets take a look at the top ten password my honeypot was seeing:

| Password | Honeypot | | MySpace | | PHPBB | | Hotmail | | RockYou | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Rank | Count | Rank | Count | Rank | Count | Rank | Count | Rank | Count |
| 123456 | 1 | 3687 | 11 | 17 | 1 | 2650 | 1 | 64 | 1 | 290729 |
| password | 2 | 2237 | - | - | 2 | 1244 | 200 | 2 | 4 | 59462 |
| test | 3 | 1470 | 862 | 2 | 12 | 223 | - | - | 166186 | 14 |
| 1234 | 4 | 1383 | 704 | 3 | 9 | 273 | 536 | 2 | 1077 | 1275 |
| root | 5 | 1320 | - | - | 1201 | 10 | - | - | 806849 | 3 |
| oracle | 6 | 1182 | - | - | 930 | 12 | - | - | 12776 | 138 |
| qwerty | 7 | 1177 | 407 | 3 | 4 | 562 | 1702 | 1 | 20 | 13456 |
| 12345 | 8 | 1136 | 703 | 3 | 5 | 418 | 53 | 4 | 2 | 79076 |
| 123 | 9 | 1078 | - | - | 14 | 216 | - | - | 3985 | 400 |
| 1q2w3e | 10 | 1022 | 700 | 3 | 105 | 48 | - | - | 1196 | 1162 |

So what do all of those numbers mean?

- The most common password on my honeypot actually is normally the most common one at the other sites as well
- The top 10 honeypot passwords appear consistently at the other sites, more when the sample size is larger
- Assuming that users do not look at leaked pasword lists to help choose a password, then the attackers are also being smart and making sure their lists are relevant
- To put it in scope: across 4 sites leaked passwords, using "12346" would have given me access to 293460 accounts

So far, so bad. But something else has also happened recently. Anonymous and a certain security company have crossed swords. This has lead to a site this company ran having it's backend database being made public. This website was very much infosec focused and was used by infosec people. So I started thinking again (never a good sign), all of these leaked passwords are common knowlegde so how many infosec people would make use of passwords on these lists?

The first thing was to get the data out into a format that could be used, and I ended up with this many users (there was no cleanup):

```
# wc -l ./list.txt
81450 ./list.txt
```

Then, very simply run that through John the Ripper with the leaked passwords from above and see how many users in that list had their passwords guessed:

```
guesses: 21337  time: 0:00:00:08 100.00% (ETA: Tue Feb 22 16:06:13 2011)  c/s: 88175M
```

So, a vanilla run through the the list showed that about a quarter of the users used passwords found on these

leaked lists. Hmmm (more thinking), John has a function to allow you to use standard mangling rules to make "smarter" guesses from a dictionary. Again, these are types of replacements/mangles which are common knowledge, would using this produce more results?

```
guesses: 23246  time: 0:00:03:53 100.00% (ETA: Tue Feb 22 16:12:52 2011)  c/s: 35386M
```

So just under 2000 more passwords were found using standard mangling techniques on the leaked password lists. As you can see, neither of these were any great computational hurdle since the first test took 8 seconds and the second took just shy of 4 minutes. But more importantly, it showed that even security people can use passwords that they know (or should know) they should not. This problem with passwords is why brute-forcing is still so popular and why it is still so successful. There are lots of guides as to what makes a good password, lots of good advice for when you have no choice but to use a password, please use it.

Public lists, leaked info, John the Ripper, all of these are readily avalible and require no great skill. Thus there is no reason why we should not use this information to help others (or at least ourselves) choose better passwords. Have fun and learn.