CHECKING PASSWORDS WITH JOHN

I have in the past spoken about passwords (see here), but the one of main problems with passwords is the people who use them. Users very often choose simple or easily guessed passwords. One of the best ways of sorting this out, is by doing a password audit. Now I know that to some people the idea of a password audit is seen as an ethical problem, but realisticly, it is very often the only way to check that your password policy is being enforced. Now in order to audit the passwords, you need to a password-cracking program, this is where "*john*" comes in...

What is Needed...
You will need to get the software of course, and I suggest getting both the latest build and also the last major build, as you will need the *.chr* files. The process should go something like this..

```
wget http://www.openwall.com/john/c/john-1.6.tar.gz
wget http://www.openwall.com/john/c/john-1.6.39.tar.gz
gzip -d john-1.6.tar.gz
tar -xvf john-1.6.tar
gzip -d john-1.6.39.tar.gz
tar -xvf john-1.6.39.tar
cd john-1.6.39
cd src
make clean generic
cd ..
cd run
cp ../../john-1.6/run/*.chr ./
```

After this is should have the *john* binary in your *john-1.6.39* folder. You can also now download any dictionary files you may want to use (google is your friend),

Lets begin...
John-the-Ripper is a very nice tool (for both sides of the fence unfortunately) in that it is fast, portable, configurable, by default can automagically handle many different password hash types and is free. Now that we have the binary to work with, lets try a simple test. I assume you are on a linux box..

```
unshadow /etc/passwd /etc/shadow > mypasswd
```

This will create the *mypasswd* file which *john* can use to try to crack the passwords..

```
john mypasswd
```

That will use just the default settings that *john* has, also if you want to see the progress, hit the <*space-bar*> while *john* is running. *John* will output the cracked passwords as it gets them, while all the background stuff is stored in the **.pot*. **.log* and **.rec* files.

Getting a little smarter
John also has some other modes which are very useful. You can use a dictionary..

```
john --wordlist=./words-english-big.dic ./mypasswd
```

You can use various text-mangling rules with your dictionary..

```
john --wordlist=./words-english-big.dic --rules ./mypasswd
```

You can use a full-everything-and-the-kitchen-sink approach (just do not expect it to finish anytime soon)..

```
john --incremental ./mypasswd
```

You can also create your own files for use by *john* as long as the follow the simple format of..

```
username:password_hash::::
```

For example if you wanted a file taken from a samba *smbpasswd* file for *John* to crack the *LanMan* hashes you could use a script like..

```
for x in `cat /etc/samba/smbpasswd | cut -f 1,3 -d ":"`
 do
  echo "$x::::" >> smb.lst
 done
```

Final Words

John-the-Ripper is a very powerful tool with many other options, for example it can also do distributed cracking using multiple servers. So it would be well worth your while to play around a bit. As always have fun and learn.