

“PASSWORD CRACKING”

--S.JOE MATHEW
(192IT159)

STEPS:

1. We are going to crack a md5 hash of a password “joe4666” any online tool to convert password to md5 hash.

Your Hash: 40287c687201a8939159989c98df4ee0
Your String: joe4666

2. We are going to use a dictionary attack with a wordlist created using cupp tool. I am installing cupp **apt-get install cupp**. I am using cupp -i . (interactive mode)

```
root@kali:~/cupp# cupp -i
cupp.py!
# Common
# User
# Passwords
# Profiler
[ Muris Kurgas | j0rgan@remote-exploit.org ]
[ Mebus | https://github.com/Mebus/ ]

[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: joe
> Surname:
> Nickname:
> Birthdate (DDMMYYYY):

> Partners) name:
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):

> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY):

> Pet's name:
> Company name:

> Do you want to add some key words about the victim? Y/[N]: 4666
> Do you want to add special chars at the end of words? Y/[N]:
> Do you want to add some random numbers at the end of words? Y/[N]:
> Leet mode? (i.e. leet = 1337) Y/[N]:
```

```
[*] Now making a dictionary ...
[*] Sorting list and removing duplicates ...
[*] Saving dictionary to joe.txt, counting 134 words.
[*] Now load your pistolero with joe.txt and shoot! Good luck!
root@kali:~# ls
abcd.gif      dll.dll      h5nlwzig.default-release  index.html.1  index.html.5  LHOST      Pictures      shikee2.exe      wireshark.html.save
abc.gif       Documents    hijack.c                  index.html.10 index.html.6   metaloder_dll  Public        shikee.exe       wireshark.html.save.1
ab.gif        Downloads    hijack.dll                index.html.11 index.html.7   metasploit-loader  PycharmProjects  shik.exe        watchdog.jpeg
a.gif         ENCODE       h180con9.default          index.html.12 index.html.8   metdll         PYMERION2.exe  simple-backdoor.php  xhr.html
backdoor      firepwd      htmlinjection             index.html.13 index.html.9   Music          remote.pcap     temp
code          ft1.exe      HTTP                      index.html.14 intro          pass.txt        samplecsv.csv    users.txt
Code          ft2.exe      httpse.exe                index.html.2  joe.txt        pademo         reverse_all.exe  Templates
Desktop       ft.exe       https.exe                 index.html.3  lfi            pay.exe        shika.exe        Videos
dll.c         GfagDIOT.jpeg index.html                 index.html.4  lfi_prependappend  pefile        shikee1.exe      wireshark.html
root@kali:~#
```

3.Here is my wordlist created and saved in joe.txt.

```
GNU nano 4.5                               joe.txt
Joe2008
Joe2009
Joe2010
Joe2011
Joe2012
Joe2013
Joe2014
Joe2015
Joe2016
Joe2017
Joe2018
Joe2019
Joe2020
Joe4666
Joe46662008
Joe46662009
Joe46662010
Joe46662011
Joe46662012
Joe46662013
Joe46662014
Joe46662015
Joe46662016
Joe46662017
Joe46662018
Joe46662019
Joe46662020
Joe4666
Joe_2008
Joe_2009
Joe_2010
Joe_2011
Joe_2012
Joe_2013
Joe_2014
```

4.To crack the password we are using john the ripper which is pre installed in kali linux . The command is : **john --format=raw-md5 /root/Downloads/joe.txt** (my word list) / **root/cupp/hash** (where the joe4666 md5 hash stored file)

```

root@kali:~/cupp# john --format=raw-md5 /root/Downloads/joe.txt /root/cupp/hash
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
0g 0:00:00:05 3/3 0g/s 525548p/s 525548c/s 525548C/s dwdeas..sharlotte
0g 0:00:00:07 3/3 0g/s 1043Kp/s 1043Kc/s 1043KC/s 19931013..19930487
0g 0:00:00:08 3/3 0g/s 1437Kp/s 1437Kc/s 1437KC/s kntigz..sockyora
0g 0:00:00:09 3/3 0g/s 1811Kp/s 1811Kc/s 1811KC/s 10248621..10233405
0g 0:00:00:10 3/3 0g/s 2111Kp/s 2111Kc/s 2111KC/s dynamss..dynaby4
0g 0:00:00:12 3/3 0g/s 2569Kp/s 2569Kc/s 2569KC/s summyboand..marias2
0g 0:00:00:13 3/3 0g/s 2866Kp/s 2866Kc/s 2866KC/s twtlcme..samon113
0g 0:00:00:14 3/3 0g/s 3106Kp/s 3106Kc/s 3106KC/s n1lr99..marisbroca
0g 0:00:01:32 3/3 0g/s 7552Kp/s 7552Kc/s 7552KC/s 9duh9w..9duwei
0g 0:00:01:33 3/3 0g/s 7565Kp/s 7565Kc/s 7565KC/s bannolee11..bannoll135
0g 0:00:01:34 3/3 0g/s 7586Kp/s 7586Kc/s 7586KC/s 80m61L..80m6MP
0g 0:00:01:35 3/3 0g/s 7597Kp/s 7597Kc/s 7597KC/s cruemh84..crue2dik
0g 0:00:02:44 3/3 0g/s 8195Kp/s 8195Kc/s 8195KC/s dyomi192..dyomph8r
0g 0:00:02:45 3/3 0g/s 8203Kp/s 8203Kc/s 8203KC/s cz0zer..cz0zk8
0g 0:00:02:46 3/3 0g/s 8214Kp/s 8214Kc/s 8214KC/s 9/lsdw..9/luk2
0g 0:00:02:47 3/3 0g/s 8220Kp/s 8220Kc/s 8220KC/s 067732591..067733195
0g 0:00:02:48 3/3 0g/s 8221Kp/s 8221Kc/s 8221KC/s i4h!^..i12=
0g 0:00:03:56 3/3 0g/s 8571Kp/s 8571Kc/s 8571KC/s matuptrs..matub1u1
0g 0:00:03:59 3/3 0g/s 8578Kp/s 8578Kc/s 8578KC/s dj0133ss..dj0196jh
0g 0:00:04:04 3/3 0g/s 8593Kp/s 8593Kc/s 8593KC/s avdeyh..avdm2q
0g 0:00:05:43 3/3 0g/s 8634Kp/s 8634Kc/s 8634KC/s 215a2yk..215a8+?
0g 0:00:05:44 3/3 0g/s 8635Kp/s 8635Kc/s 8635KC/s a7psb9..a7vih6
0g 0:00:06:29 3/3 0g/s 8620Kp/s 8620Kc/s 8620KC/s cowcp5r..cowms49
0g 0:00:06:30 3/3 0g/s 8622Kp/s 8622Kc/s 8622KC/s jlgua3n..jlgubm2
0g 0:00:06:31 3/3 0g/s 8624Kp/s 8624Kc/s 8624KC/s rru1fda..rru24bl
joe4666 (?)
1g 0:00:07:03 DONE 3/3 (2020-06-26 11:34) 0.002362g/s 8698Kp/s 8698Kc/s 8698KC/s joe43r0..joe4623
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed

```

Here we can see 'joe466 (?)' This is a password from my hash and wordlist.

---thank you