CYSE 301: Cybersecurity Technique and Operations

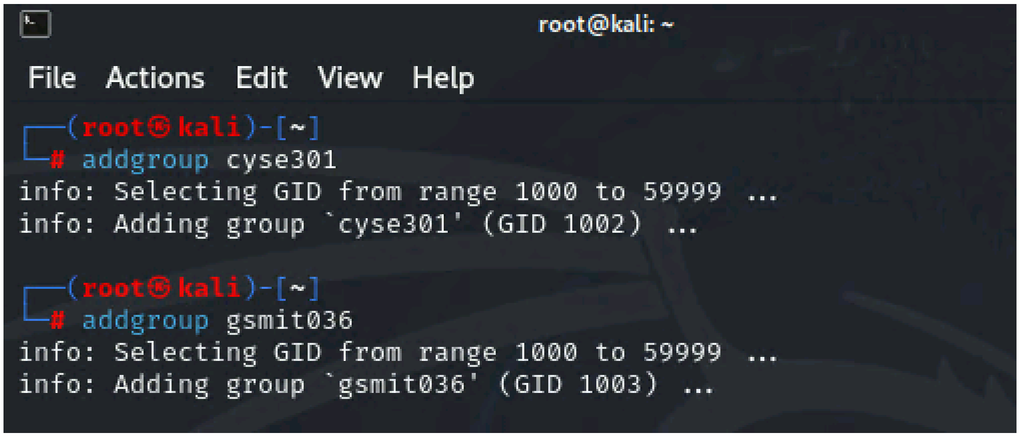
Assignment 5: Password Cracking (Part A)

BY: Trey Smith

At the end of this module, each student needs to submit a report that includes the solutions to the following tasks. Make sure you take a screenshot for every single step as proof. You need to use

Task A: Linux Password Cracking (25 points)

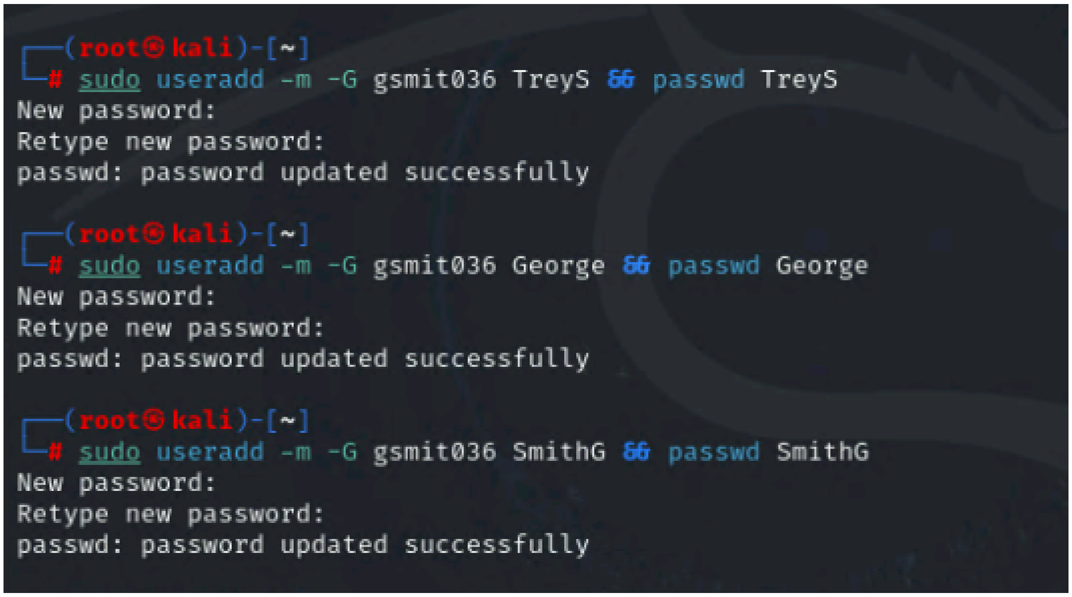
1. **5 points.** Create two groups, one is **cyse301**, and the other is your ODU Midas ID (for example, svatsa). Then display the corresponding group IDs.



```
┌──(root㉿kali)-[~]
└─# addgroup cyse301
info: Selecting GID from range 1000 to 59999 ...
info: Adding group `cyse301' (GID 1002) ...

┌──(root㉿kali)-[~]
└─# addgroup gsmit036
info: Selecting GID from range 1000 to 59999 ...
info: Adding group `gsmit036' (GID 1003) ...
```

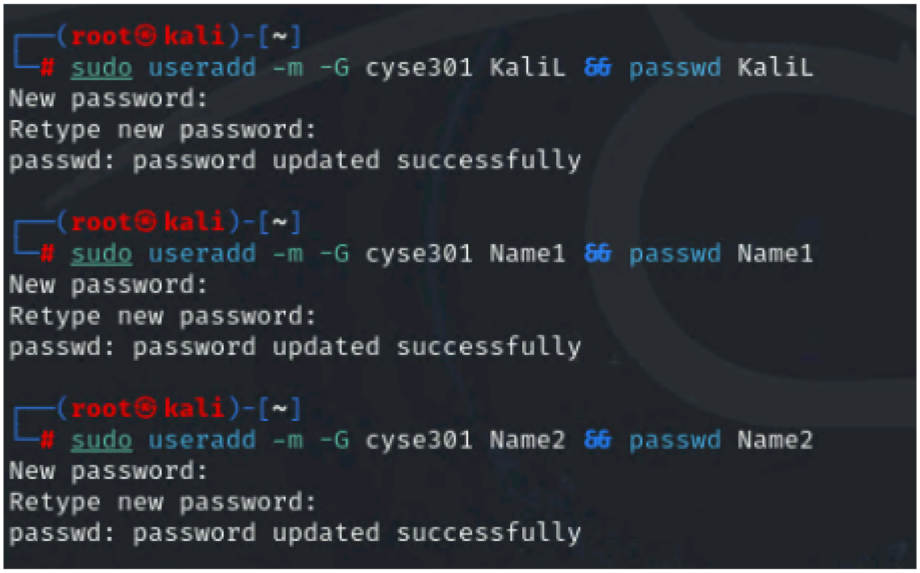
2. **5 points.** Create and assign three users to each group. Display related UID and GID information of each user.



```
┌──(root㉿kali)-[~]
└─# sudo useradd -m -G gsmit036 TreyS && passwd TreyS
New password:
Retype new password:
passwd: password updated successfully

┌──(root㉿kali)-[~]
└─# sudo useradd -m -G gsmit036 George && passwd George
New password:
Retype new password:
passwd: password updated successfully

┌──(root㉿kali)-[~]
└─# sudo useradd -m -G gsmit036 SmithG && passwd SmithG
New password:
Retype new password:
passwd: password updated successfully
```

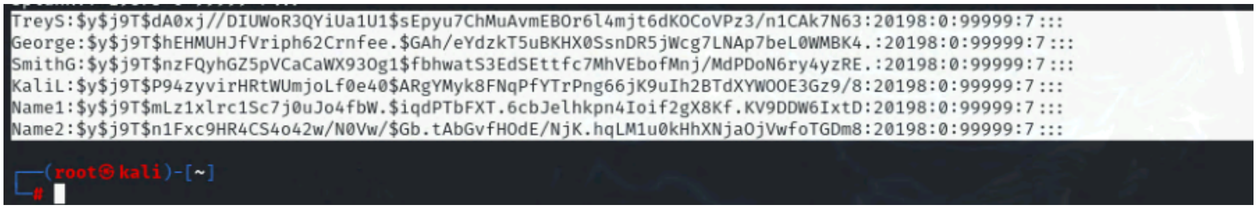


```
┌──(root㉿kali)-[~]
└─# sudo useradd -m -G cyse301 KaliL && passwd KaliL
New password:
Retype new password:
passwd: password updated successfully

┌──(root㉿kali)-[~]
└─# sudo useradd -m -G cyse301 Name1 && passwd Name1
New password:
Retype new password:
passwd: password updated successfully

┌──(root㉿kali)-[~]
└─# sudo useradd -m -G cyse301 Name2 && passwd Name2
New password:
Retype new password:
passwd: password updated successfully
```

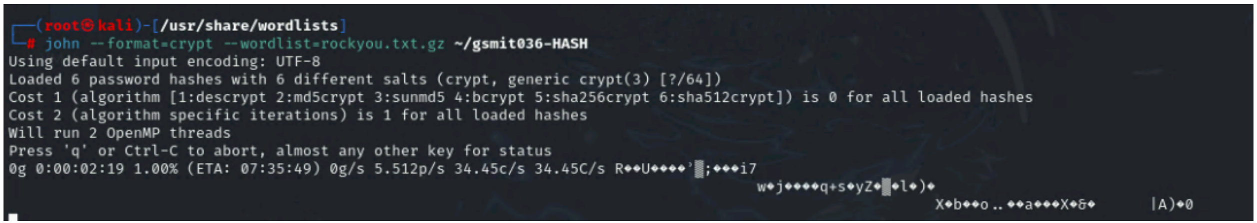
3. **5 points.** Choose Three new passwords, **from easy to hard**, and assign them to the users you created. You need to show me the password you selected in your report, and **DO NOT** use your real-world passwords.



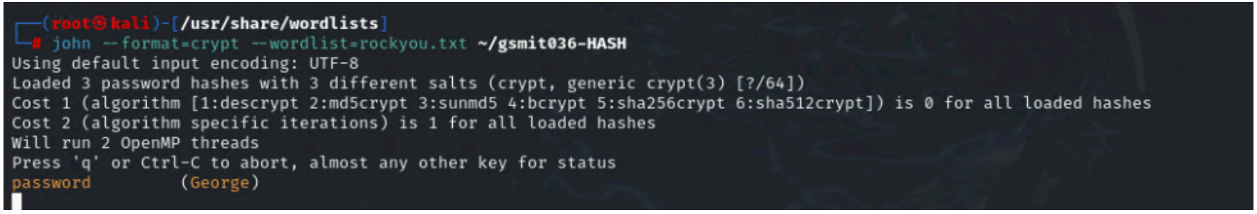
```
TreyS:$y$j9T$dA0xj//DIUWoR3QYiUa1U1$sEpyu7ChMuAvmEBOr6l4mjt6dKOCoVPz3/n1CAk7N63:20198:0:99999:7:::
George:$y$j9T$hEHMUHJfVriph62Crnfee.$GAh/eYdzkT5uBKHX0SsnDR5jWcg7LNAp7beL0WMBK4.:20198:0:99999:7:::
SmithG:$y$j9T$nzFQyhGZ5pVCaCaWX93Og1$fbhwatS3EdSEttfc7MhVEbofMnj/MdPDoN6ry4yzRE.:20198:0:99999:7:::
KaliL:$y$j9T$P94zyvirHRtWUmjoLf0e40$ARgYMyk8FNqPfYTrPng66jK9uIh2BTdXYWOOE3Gz9/8:20198:0:99999:7:::
Name1:$y$j9T$mLz1xlrc1Sc7j0uJo4fbW.$iqdPTbFXT.6cbJelhkpn4Ioif2gX8Kf.KV9DDW6IxtD:20198:0:99999:7:::
Name2:$y$j9T$n1Fxc9HR4CS4o42w/N0Vw/$Gb.tAbGvfHOdE/NjK.hqLM1u0kHhXNjaOjVwfoTGDm8:20198:0:99999:7:::

┌──(root㉿kali)-[~]
└─# █
```

4. **5 points.** Export all Three users' password hashes into a file named "**YourMIDAS-HASH**" (for example, svatsa-HASH). Then launch a dictionary attack to crack the passwords. You MUST crack at least one password in order to complete this assignment.



```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# john --format=crypt --wordlist=rockyou.txt.gz ~/gsmit036-HASH
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:02:19 1.00% (ETA: 07:35:49) 0g/s 5.512p/s 34.45c/s 34.45C/s R◆◆U◆◆◆◆'▒;◆◆◆i7
                                                                                         w◆j◆◆◆◆q+s◆yZ◆█◆l◆)◆
                                                                                                               X◆b◆◆o..◆◆a◆◆◆X◆&◆      |A)◆0
▪
```



```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# john --format=crypt --wordlist=rockyou.txt ~/gsmit036-HASH
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (George)
█
```

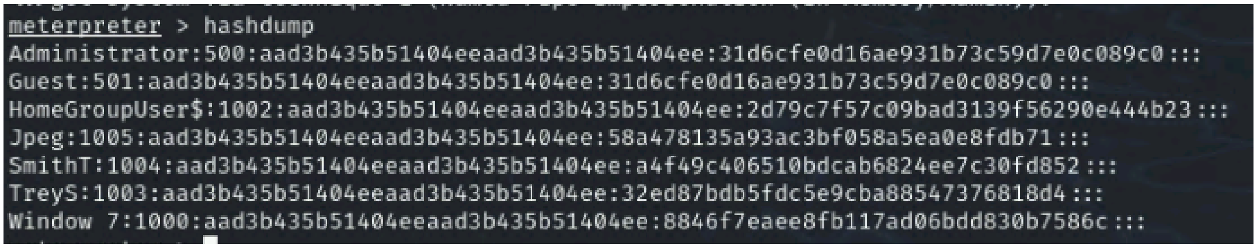
restarted it 5 times and changed some things around but I finally got it.

Task B: Windows Password Cracking (25 points)

Log on to Windows 7 VM and create a list of 3 users with different passwords (OR you may create users using net users \add command as you did in lab-4-task-c). Then you need to establish a reverse shell connection with the admin privilege to the target Windows 7 VM.

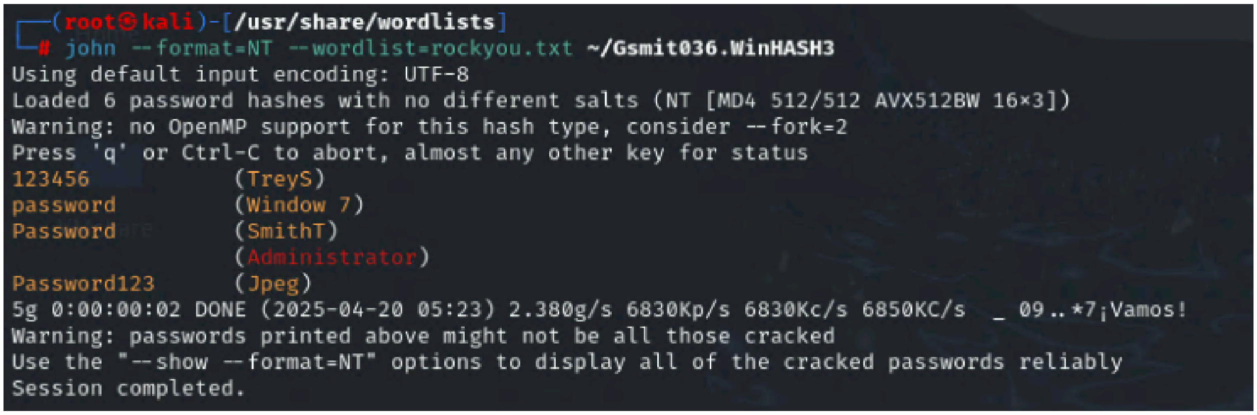
Now, complete the following tasks:

1. **5 points.** Display the password hashes by using the "hashdump" command in the meterpreter shell. Then



```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
Jpeg:1005:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
SmithT:1004:aad3b435b51404eeaad3b435b51404ee:a4f49c406510bdcab6824ee7c30fd852:::
TreyS:1003:aad3b435b51404eeaad3b435b51404ee:32ed87bdb5fdc5e9cba88547376818d4:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
```

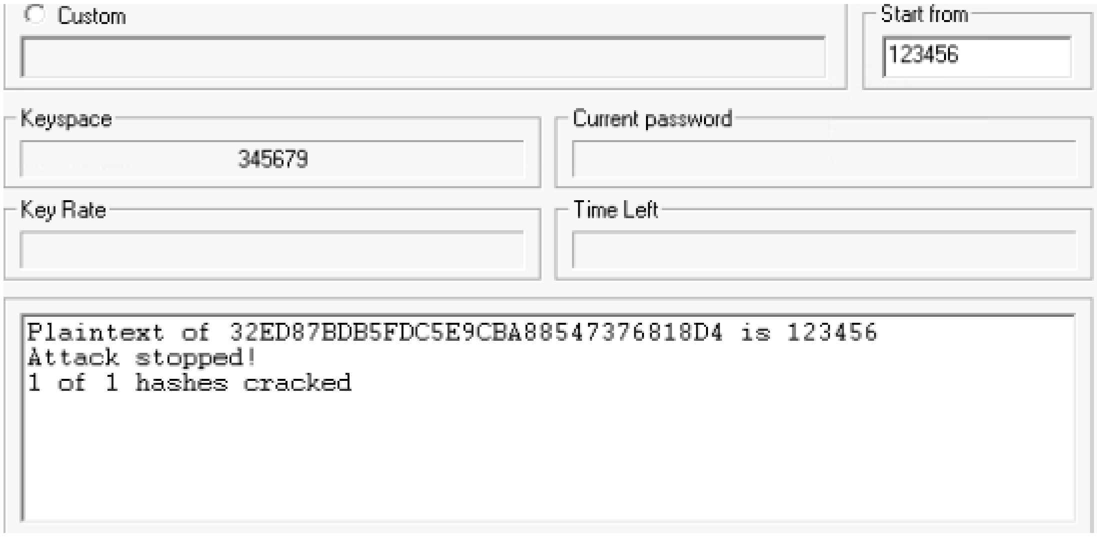
2. **10 points.** Save the password hashes into a file named "**your_midas.WinHASH**" in Kali Linux (you need to replace the "your_midas" with your university MIDAS ID). Then run **John the ripper** for **10 minutes** to crack the windows users' passwords (You MUST crack at least one password in order to complete this assignment.).



```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# john --format=NT --wordlist=rockyou.txt ~/Gsmit036.WinHASH3
Using default input encoding: UTF-8
Loaded 6 password hashes with no different salts (NT [MD4 512/512 AVX512BW 16×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
123456           (TreyS)
password         (Window 7)
Password         (SmithT)
                 (Administrator)
Password123      (Jpeg)
5g 0:00:00:02 DONE (2025-04-20 05:23) 2.380g/s 6830Kp/s 6830Kc/s 6850KC/s _ 09..*7¡Vamos!
Warning: passwords printed above might not be all those cracked
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Had to change the format type

3. 10 points. Launch/open the password cracking tool, **Cain and Abel** in Windows 7 VM, via a remote desktop window. Then, implement BOTH brute force and dictionary attacks to crack the passwords for Windows7 users. (You MUST crack at least one password in order to complete this assignment).



○ Custom

Start from: 123456

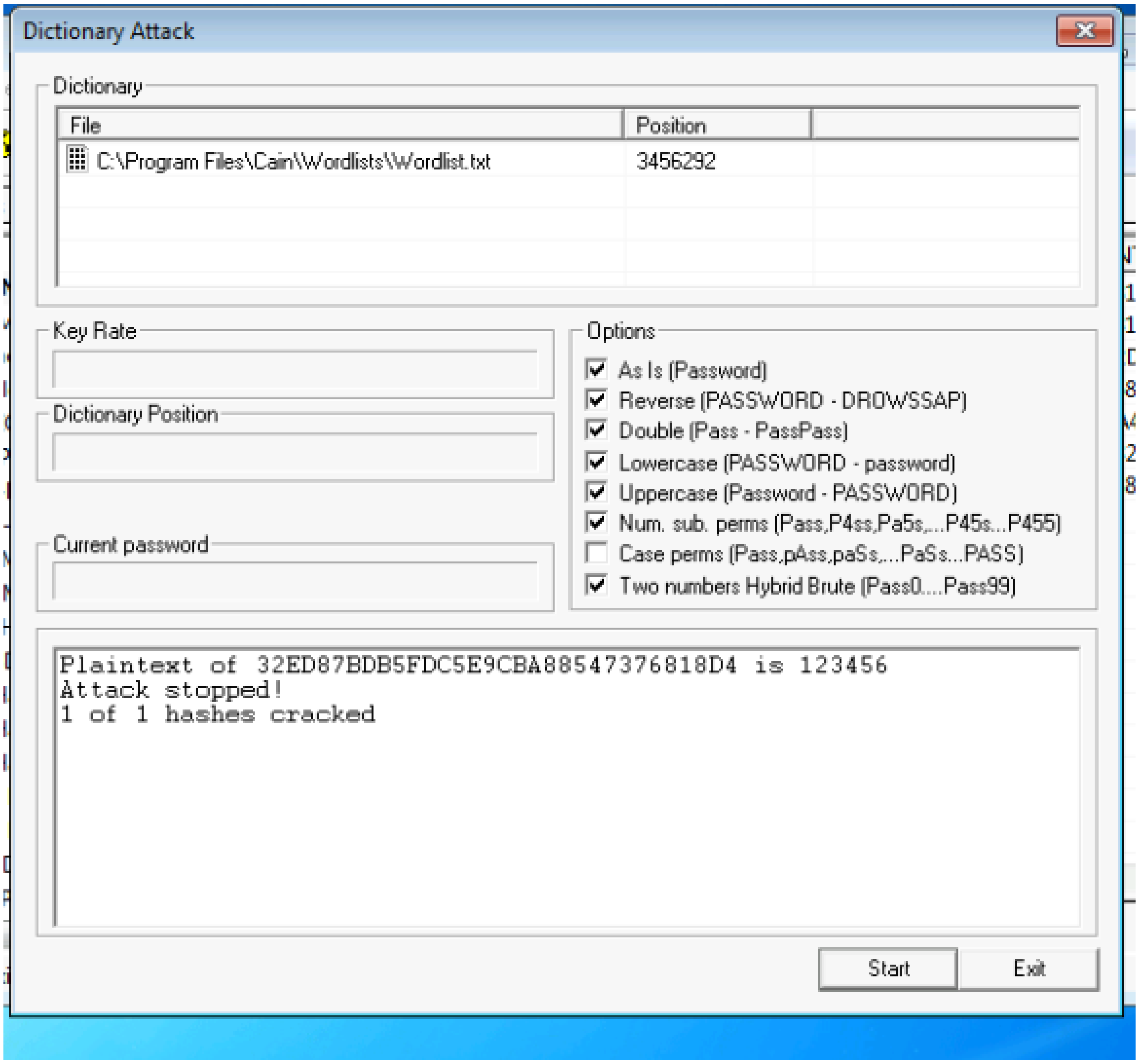
Keyspace: 345679

Current password:

Key Rate:

Time Left:

```
Plaintext of 32ED87BDB5FDC5E9CBA88547376818D4 is 123456
Attack stopped!
1 of 1 hashes cracked
```



Dictionary Attack

Dictionary

File	Position
C:\Program Files\Cain\Wordlists\Wordlist.txt	3456292

Key Rate:

Dictionary Position:

Current password:

Options

- ☑ As Is (Password)
- ☑ Reverse (PASSWORD - DROWSSAP)
- ☑ Double (Pass - PassPass)
- ☑ Lowercase (PASSWORD - password)
- ☑ Uppercase (Password - PASSWORD)
- ☑ Num. sub. perms (Pass,P4ss,Pa5s,...P45s...P455)
- ☐ Case perms (Pass,pAss,paSs,...PaSs...PASS)
- ☑ Two numbers Hybrid Brute (Pass0....Pass99)

```
Plaintext of 32ED87BDB5FDC5E9CBA88547376818D4 is 123456
Attack stopped!
1 of 1 hashes cracked
```

NOTE: Please refer to the class lecture to learn how to add users in windows7 and using Cain tool for windows password cracking.

Extra credit: (10 points)

Search the proper format in John the Ripper to crack the following **MD5** hashes (use the ***--list=formats*** option to list all supported formats). Show your steps and results.

1. 5f4dcc3b5aa765d61d8327deb882cf99
2. 63a9f0ea7bb98050796b649e85481845