Assignment 1 Sliding Part

As group 1, the Unix hashes we are supposed to crack are:

$1$03eQhEHr$VzfRY6Dc9MDNjKfTB8L/d0
1XRlLIqNU$PGziquQO.U2cYYkpjWZOS.
1z1Nk0xyf$sp/CDlMQNxhKw1Mn3kWmN.
1ENqxo5u0$81tdi0P3MAN9vAvUGHn6y.
$1$0gs0ZeaS$mAbjqR8ckVRYHCCHMRTBg.

The actual passwords are:

flavius$aetius
UNKNOWN
misbehavior
UNKNOWN
UNKNOWN

Only the first and third is successfully cracked using word lists; the *Roman General* one requires additional connectors (_, $, %) to be added to each name in the word list file to work properly.

The commands used are:

```
cd a1sliding
run/john --wordlist=list/roman.txt --rules hashes.txt
run/john --wordlist=list/11letterwords.txt --rules hashes.txt
run/john --show hashes.txt
```

where *hashes.txt* is the text file containing only the Unix passwords.

The Windows hashes we are supposed to crack are:

D5D8E24F574290F9302D113D646B368F:9BA8384BD50192588AFF5F9B5F9625F0
8AFC234E5BE7BB568963805A19B0ED49:9C9607EBF3287C06876D8FC44FDC711E
F4C310F5B3FAC8D63B1217229AE349BC:CB71BC560D760E506D1E96010DFDA970

The actual passwords are:

UNKNOWN
gondolier
UNKNOWN

Similar to the Unix hashes, only word lists are used to crack the second hash.

The commands used are:

```
run/john --wordlist=list/9letterwords.txt -format=LM --rules first_half.txt
run/john --wordlist=list/9letterwords.txt -format=nt --rules second_half.txt
```

In this case, the three Windows hashes are break into two separate files named *first_half.txt* and *second_half.txt* because the encryption schemes used are different for each portion of the Windows hashes.

Explanation

All 3 cracked password hashes are variations of English words that can be easily tried one by one given a dictionary file; therefore they are all weak passwords. One of the Unix and Windows passwords are composed entirely of alphanumeric letters and no result has been returned from *john the ripper* (running *incremental mode*) up until the deadline of this sliding part since they are very computationlly expensive to try out all possible permutations even length is known.

For the passwords that we have cracked, the Windows one (*gondolier*) and the 11-letter word password of Unix (*misbehavior*) are easier to crack than the *Roman General* password of Unix (*flavius$aetius*) because the former two can be *directly* cracked given word lists; however, for the *Roman General* case, each name needs to apply *three* different modifications based on the connectors.

Part 1

NOTE:
The actual user names for both machines are in all lower case.

The passwords we used are listed in the table below:

Platform	Administrator/Root Password	User1 Password	User2 Password
Linux	9%0byu(zY	v1-#>;/jf	9up]~{}z@qm
Windows	sCSsd54>ttH	O3gmDtc	mPrm8hbeenUsG

Part 2

The passwords for the Linux machine are chosen to be composed entirely of random alphanumveric letters due to the fact that the only feasible way to crack the random alphanumeric password hashes for the sliding part of assignment 1 is to use the *brute force* incremental mode of *john the ripper* program, which is the most computationally expensive to calculate due to the large number of permutations to try one by one.

For the Windows machine they are memorable sentences using a combination of alphanumeric letters and a symbol in one case. Windows Admin password is derived from “some Computing Science students don’t Sleep for more then thirty

hours". Windows user1 is derived from "Our third group member Dropped the course". Windows User2 is derived from "my Poor room mate has been Unemployed
since Graduation".

Windows web server is done through the addition of a module called mod_auth_sspi
where it can pull windows credentials from the OS directly. This allows it to edit the web server config file that can require the login credentials from the user depending on which directory that they are trying to access.

Linux FTP and TFTP servers are configured to run under the supervision of the *inetd* daemon; the configuration file for FTP server resides in */etc/* and
is named as *vsftpd.conf*, the configuration file for TFTP server is at */opt/opentftpd/opentftp.ini*.

Part 3

Reference

- Choosing Secure Passwords
- `man 1 passwd`

Division of Workload

The Windows HTTP server was set up by Stephen Arychuk, he also wrote the IP
table rules for part 3 and the report section for it; the sliding part of assignment 1 was done by Jiahui Xie, he set up the Linux FTP/TFTP server and
wrote relevant reprot section.