**CPE 449/549: Introduction to Cybersecurity Engineering**

**Lab 1: Password Cracking**

**Objective:** Use a dictionary attack to crack Linux Passwords.

***Background Information:***

1. Linux Password Storage: http://techlister.com/linux/linux-how-to-change-the-hashing-algorithm-on-linux-system/796/
2. Windows Password Storage: http://techgenix.com/how-cracked-windows-password-part1/
3. John the Ripper Password Cracker: http://openwall.info/wiki/john/tutorials
4. Implementation of SHA512-crypt vs MD5-crypt: http://www.vidarholen.net/contents/blog/?p=33

Steps:

1. Write a Python script to perform a dictionary attack on a Linux password file.
   1. Copy /etc/shadow file to your local directory. Study the format of this file.
   2. Add the following 3 lines to the /etc/shadow file. For speed purposes remove all other lines.

tommy:$6$HFQQdE2g$g0eyz6UN.c4Pg1tiQgdPPPXdQ1fEOwttCwzSah/Jo4RE9Eac4H7pgksaNLI/WSIyN8tNtCX4NaAq6Uwz.o.4W1:17400:0:99999:7:::

mathis:$6$niptplk1$.mMMVx4T375WhFkDN5RWEaD93HcmDCx3aBQrn2ZalbiRpl4FB2Rww/BeCPEfSYbegjPvoHM2llQmk/VBbSxWj.:17400:0:99999:7:::

tristan:$6$MWwusFJx$KCoO1wiWKtE.7j/7UiwD.1jXmOckMb5X4GGt1DotLS0laXdFga5n3wGfu43FC/Opxki7mY6Yf9XT.cBGN.pkp0:17400:0:99999:7:::

* 1. Use the “crypt” library crypt function to create your hash.
  2. Use the “hmac” library compare\_hash function to compare hashes from the /etc/shadow file to the hashes produced from your guesses.
  3. Use the string split() function to separate the separate the password lines from the shadow file by the ‘:’ delimiter to isolate the userid and the hash from an entry in the shadow file.
  4. Calculate the appropriate hash (using the method specified for the entry from the shadow file) for each word in this wordlist (<http://www.openwall.com/passwords/wordlists/password-2011.lst>), compare the hash, and stop comparing when you find a match.
  5. Attempt the dictionary attack for each entry in the shadow file.
  6. Remember you need to provide the word from the dictionary, the method, and the salt to the crypt() function.
  7. Print the userid and password when a match is found:  
     “Match found for userid [userid]. Password = [password]”
  8. Print the “No match was found for [userid]” when there no match in the dictionary.