Lab 2
Password Cracking with John

Goals:

1. Familiarize with Linux filesystem and known files and directories storing information related to passwords.
2. Use John The Ripper password cracking for simple dictionary attacks and more complex, combination attacks.
3. Learn about Hydra password cracking tool.

Preliminary Information:

Passwords help to secure systems running Linux and UNIX operating systems. If an attacker is able to get the root password on a Linux or UNIX system, they will be able to take complete control of that device. The protection of the root password is critical.

passwd – User accounts on a Linux system are listed in the passwd file which is stored in the /etc directory. The passwd file has less restrictive permissions than the shadow file because it does not store the encrypted password hashes. On most Linux systems, any account has the ability to read the contents of the passwd file.
shadow – The shadow file also stores information about user accounts on a Linux system. The shadow file also stores the encrypted password hashes, and has more restrictive permissions than the passwd file. On most Linux systems, only the root account has the ability to read the contents of the shadow file.
auth.log – This log file tracks SSH, or Secure Shell, connections. It provides information such as IP addresses, and date and time stamps. It also tracks other events related to security, such as the creation of new user's accounts and new group accounts.
John the Ripper – John the Ripper is an extremely fast password cracker that can crack passwords through a dictionary attack or through the use of brute force.

Part 1: Simple Password Attack

1. Start up your Kali VM.
2. To view the contents of the passwd file, type: `cat /etc/passwd`
3. View the permissions on the /etc/passwd file by typing the following command:
   `ls -l /etc/passwd`
4. Explain these permissions in your own words in your report.
5. To view the contents of the shadow file, type: `cat /etc/shadow`
6. To create a new user named yoda, type the following command in the terminal:
   root@bt:~# useradd yoda
7. To create a new user named chewbacca, type the following command in the terminal:
   root@bt:~# useradd chewbacca
8. Now, view the changes made to the passwd file by typing the following: root@bt:~# tail /etc/passwd

9. Explain the fields of /etc/passwd in your report
10. Next, examine the alterations to the shadow file by typing the following: root@bt:~# tail /etc/shadow
11. Why is there a "!" in place of a password for the new users?
12. Examine the entries in the auth.log related to account changes by typing: root@bt:~# tail /var/log/auth.log
13. What information does this log give you about the new users?
14. Set yoda's password to green by typing green, followed by Enter twice after using the command: root@bt:~# passwd yoda
15. Set chewbacca's password to green by typing green, followed by Enter twice after using the command: root@bt:~# passwd chewbacca
16. Next, examine the alterations to the shadow file by typing the following: root@bt:~# tail –n 2 /etc/shadow
17. Why are the two hashes different even though the passwords are the same?
18. Examine the entries in the auth.log related to account changes by typing: root@bt:~# tail /var/log/auth.log
19. To look for specific information about password changes within auth.log, type: root@bt:~# cat /var/log/auth.log | grep changed
20. Now it is time to use John the Ripper!
21. Lookup the command that will crack the /etc/shadow file.
22. Where are the passwords stored? (Hint: default John software file)
23. Set chewbacca's password to computer by typing computer twice after typing: root@bt:/pentest/passwords/john# passwd chewbacca
24. Now use a wordlist like rockyou or wordlist to crack /etc/shadow. The wordlist is in a specific folder in your Kali distribution (find this! Do not download it again!)

Part 2: Complex Password Attack with Substitution and Multiple Dictionaries

For this part of password cracking, you will use the following hashes:

```
$1$SPLFK6cT$eyS3cHwC1nK67koa8iwM80
$1$aPAO6qe9$x25sKDTUho58jg9AYnamN/
$1$92y/OxK/$f2eF.WTF7a3AbhI7vTjkY1
$1$eQd41u8Z$CAkXiDcBRLEaIzjmCc9j70
```

Your hint about this passwords is: "Pokemon".

1. The passwords have the following substitution rules:
    a. Substitute o with 0 (zero)
    b. Substitute e with 3
    c. Substitute s with 5
    d. Substitute a with @
2. Based on the above, use John to crack these passwords. Use john rules and commands. Paste these in your report.
3. Note: you will need to try all the combinations of the substitution rules. Do not forget that names start with a capital.

Sources:

http://lpc1.clpccd.cc.ca.us/lpc/mdaoud/CNT7501/NETLABS/Ethical_Hacking_Lab_08.pdf