Password Cracking Lab

We just learned that hash functions are one-way algorithms, ideally with a unique output correlating to a unique input. What if a hacker had both the hash code, or output, and knowledge of what kind of algorithm computed the hash? Using brute force, one could compute the hash code of infinite input possibilities comparing the output to the known hash code. With a match, the hacker has magically found the input.

This is the concept of cracking passwords. Windows and Linux computers both store local copies of hash output of the computer users' passwords used to validate the correct password. Using these hash codes along with the knowledge of what algorithm the Operating Systems use, one can find users password. Conveniently, Linux commands easily available populate a list of well-known passwords and can automatically crack the passwords of both Windows and Linux hash codes. Recently, Windows 10 updates have made the process of obtaining their hashes much more difficult, so we will complete this lab in Linux. I did this in a Kali Virtual Machine. I have included log files with my command line history showing the process for help. View these easily

This lab is completed in the terminal and assumes general knowledge of Linux commands. This link can help you catch up to speed.

http://linuxcommand.org/lc3_learning_the_shell.php

Workstation Download (virtual machine host)-
https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html

Kali Download - https://www.kali.org/downloads/

Steps:

1. Install Kali Linux on a virtual machine.
2. Once installed, open a terminal.
3. Add a few new users on the system using the command ***adduser.*** The name can be any user you wish. Choose passwords ranging from poor choices (I used "password"), to more sophisticated passkeys. Restart Kali for users to take effect.
4. Once users are created, navigate to */etc* directory. Copy "shadow" and "passwd" out of this directory to another place. I placed my files in the root directory.
5. From here, you can use a tool in John the Ripper's toolset called *unshadow* to combine the "shadow" and "passwd" file into a usable format for John the Ripper to crack. Make sure you are in the directory with the copied files. (Note, this process is needed because Linux salts their password hashes. For more

information, here's the wiki page on salts - https://en.wikipedia.org/wiki/Salt_(cryptography))

sudo unshadow <passwd> <shadow> > <hashes.txt>

6. Now let's get a word dictionary to compute hashes. Kali Linux has a pretty good password wordlist included that we will unzip to a text file:

   zcat /usr/share/wordlists/rockyou.txt.gz > <wordlist.txt>

7. Run john to find the password. Use man to view options. For trickier passwords it may help to add more rules like "-rules=Jumbo". Use *man* to learn more about john the ripper options.

   john <hashes.txt> -format=sha512crypt -wordlist=<wordlist.txt>

NOTE: While I won't step through this, you can also try to complete in Windows. Without knowing what version of windows used, I cannot guarantee success:

To find Windows passwords, boot Kali Linux from a flash drive on the Windows machine (This overcomes permissions associated with copying and viewing the hashes). Mount the windows hard drive, and copy "SYS" and "SAM" files from the Windows/System32/config directory. They contain the hash codes. Run *samdump2 SYS SAM -o <output.txt>* to create hash file that John the Ripper can use. Now use John with *-format=NT* for the windows hash algorithms. All other commands, like generating a word list, still apply.