Password cracking

Windows password recovery

1. You have inadvertently forgotten your Windows password and can't log in to your system. You really need to obtain access to your system. You also need to figure out passwords for others in the system. You can use either VirtualBox or the VM Farm.

VirtualBox

The windows image is available (only on campus) here.

After you have copied it, extract it, and open VirtualBox, create a new vm, DON't add any disk to it. Then go into settings->storage->remove the sata controller. Add an IDE controller. Add the hard disk you just copied to the IDE controller. Make sure that windows boots, verify that the user `joe` is password protected, then shut it down normally.

NOTE: When booting from a disk drive, just add an iso as optical storage under VirtualBox storage settings. Now boot the vm. (You may have to double check that the boot order finds the optical disk prior to the hard disk under System Settings within VirtualBox)

You will need a Hiren's boot cd. Download.

VMFarm

The image you should clone is called `it4510-passcrack`. I gave mine 4096M Ram (via the citv command-line)

To boot from a disk drive, make sure you select the `d` drive at boot time. You will boot from the hirens option.

General Instructions

You could probably guess a few passwords pretty easy, but let's find a tool that will do a few things for us. You should NOT boot windows in safe mode.

- One easy way to regain access to the system is simply resetting the password or blanking it out.
  - Here is a way to do it movie
  - reboot
- Take a screenshot(s) showing that you did this and that you can login as the user `joe`.

Obviously you could do anything now that you are an administrator, but don't. Let's crack a few passwords.

First, login with the vagrant user. If you can't guess the password, blank it out like you did with the joe user.

Windows password hash crack

It is fairly trivial to reset a users password as we did above, but what if you want to find out the password. As you are logged in as the vagrant user, you should see an `ophcrack` on the desktop. I have already downloaded a rainbow table in the `Downloads` directory that you could add. Add the local sam file, start the crack. See how many passwords you can find. If ophcrack isn't loading the sam file, the sam file probably got corrupted from the last part. Delete this vm, re-clone, and login as the vagrant user (password is `vagrant`).

Take a screenshot.

Linux password recovery

For this assignment, we will make the assumption that you have physical access to a linux machine and that you have pulled off the `/etc/passwd` file and the `/etc/shadow` files and put them in the correct format so that your password cracking tool can work. This file is located at here (only on-campus)

1. You are welcome to use any tools you can find. The objective is to retrieve passwords.

- On an ubuntu system, `sudo apt-get install john` (this is also installed the machine you logged into for project 1)
- The performance of running john on the virtual machines is poor, if install john on a *real* machine, you should have better performance.
- You should do something like `john file.to.crack` and sit back and let john do its' stuff.
- I found that it was able to crack 2 of the passwords in less than 5 minutes. You could just leave the process running and come back in a day or so and see if you were able to crack some more. (When I came back the next day it had cracked an additional 2 passwords)
- John didn't alert me when it found a password, so I killed it after a few minutes and did `john --show file_to_crack_2015.txt`. And it showed me what it had found.

2. Take a print screen of your cracking abilities. (I expect that you will have at LEAST 1 cracked password on the Linux machine)

Online password attack

I have a test machine set up at 144.38.193.245. You should attack the ftp service using hydra to see if you can crack the password for `steve` and `fred` and `betsy`. (The last one is the hardest). You should use this password file. Please record a print screen of the ultimate password results. Hydra runs something like this:

```
    hydra -l username -P password_list.txt 144.38.193.245 ftp
```

Your results should look something like this (though you WON'T have xxxx's for the password):

```
    [22][ssh] host: 144.38.204.41   login: fred   password: xxxxxxxxxx
    [STATUS] attack finished for 144.38.204.41 (waiting for children to finish)
```

Hydra is also installed on the machine from lab 1.

To Submit

- Prove to me that you did all of the above. (Maybe some print screens, or other descriptions)
- List all the users with their passwords (as much as you were able to decipher)
- One document please (preferrably PDF). No zip or tar.