Privilege Escalation

Linux Password Recovery

You have inadvertently forgotten your Linux 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 are NOT required to find all other user passwords, just the ones mentioned below.

Virtualbox users will need to obtain the image

VM Farm users will need to clone the machine `it4510-ubuntu-1404`.

If you boot it, you won't be able to login since you don't have any password. Instead of booting it normally, boot it in recovery mode. This is under advanced options in the grub boot menu. In recovery mode, you should be able to drop to a shell in the root filesystem (maybe something like `/dev/sda1`). The system is booted in readonly mode, if you execute the command `mount -o remount,rw /` it will remount in writable mode. You should be able to find what users exist in the system. (Hint: look in /etc/passwd). To blank a users password, you essentially delete the hash in `/etc/shadow`. Careful not to delete any of the other fields or colons (:).

You should blank the password for the `rubio` user.

Then, reboot and see if you can login as the `rubio` user. Take a screenshot being logged in as the `rubio` user. (I know you could give any user root permissions here, but let's pretend we can't)

Cracking

As you are hopefully now logged in, you can see what other users exist. You could use john to try and crack the passwd file, but as we have already done this, let's skip it.

Escalating

This system has at least 3 setUID vulnerabilities. See if you can figure out how to exploit 2 of them. Here are some potential resources:

- here
- here

Take screenshots of what you did to get root.

Hint: vim.basic has a setuid vulnerability, so basically, you can now edit `/etc/sudoers` and add rubio in the user specification setting. You will have to save your changes in vi with `:w!`. Then, as the rubio user, you should be able to do a `sudo bash` and get a root shell (A root shell ends with a #).

Online password attack

Once you have root privileges, you can edit your network settings so that your machine can connect to the internet. On this system, you will edit the `/etc/network/interfaces` file. Essentially change the word dhcp to static and add lines like this:

```
    iface eth0 inet static
        address 10.1.1.125
        netmask 255.0.0.0
        gateway 10.1.1.1
        dns-nameservers 144.38.192.2
```

Yours might not be eth0, it might be ens3 or something. Obviously change the addresses to those that are relevant for you. You either need to restart the machine or run `sudo /etc/init.d/networking restart` for the networking changes to take effect.

Use hydra to attack the ssh port of your machine. You should be able to crack the password for `curtis` and `tom` using the password list from the previous assignment. You should be able to find how to run the hydra command to attack your ssh port by searching on google.

Virtualbox users: The easiest way to run hydra against the vm will be to create a second vm that has hydra installed. I recommend using the most current version of Kali linux. You can then see the ip address of your vms with `ip a`. You may need to modify some network stuff from Virtualbox. Using Kali, you could also do a `netdiscover` command to find other machines on your network.

Take screenshot of discovered passwords.

To Submit

- Prove to me that you did all of the above. (Maybe some print screens, or other descriptions)
- One document please (preferrably PDF). No zip or tar.