CS312 :: Homework 8

Answer the following questions. You'll need to use Kali and its tools, along with reviewing the Kali lecture, to answer these questions.

Setup

Download these virtual machines from Canvas:

1. pfSense_Reference
2. Kali_Reference
3. Alpine_Kali_HW
4. Metasploitable_HW

Make sure that the network settings of these are as follows:

- pfSense_Reference:
  - Adapter 1: NAT
  - Adapted 2: Internal Network: CS312LAN
- Kali_Reference:
  - Adapter 1: Internal Network: CS312LAN
- Alpine_Kali_HW
  - Adapter 1: Internal Network: CS312LAN
- Metasploitable_HW
  - Adapter 1: Internal Network: CS312LAN

Start up the virtual machines listed above, router first. Make sure that the pfSense router is fully up and running before starting the others!

The Situation

For question 3, you'll need to know the story:

You had a keylogger and backdoor on the Alpine_Kali_HW VM, but it was discovered and removed! Before your malware was uninstalled, though, it weakened the system. At this point, the situation is:

- There are two user accounts: "root", and "lowlevel". The root account has superuser privileges, but the lowlevel account does not. You do not know the password to either, anymore.
- Your malware added a public RSA SSH key to /home/lowlevel/.ssh/authorized_keys on the Alpine_Kali_HW VM!
- You have the matching private RSA SSH key stored on Canvas, currently called "id_rsa.kalihw" (a link to it is in this assignment on Canvas). It'll need to be renamed "id_rsa" to be useful, and must be placed into the `~/.ssh` folder of the account on the Kali VM you use (probably `/root/.ssh`, which may not exist until you create it). Further, note that you need to "`chmod 600 id_rsa`" that key, once it's in place, for SSH to be able to use it.
- Your malware changed the permissions of the /etc/shadow file such that the lowlevel account can read it.

Questions

1. `hashcat`, the password cracker, has a mode called "straight", with id zero. This mode simply tries all the words in the dictionary that you provide on execution. What other kinds of attack modes does `hashcat` have? *(3 points)*
2. What are the contents of a file named “`secrets`”, which file is stored somewhere on the Metasploitable_HW VM? *(10 points)*
3. These questions are about information on the Alpine_Kali_HW VM:
    a. What is the “lowlevel” account password? *(6 points)*
    b. What is the “root” account password? *(6 points)*
    c. What are the contents of the file located at `/root/secrets`? *(15 points)*