Daria Marochnik

Extra Credit Assignment #1

1. Attach the Android VM hard disk in second position on the Kali Linux VM.
2. Start your Kali Linux machine. Type the command mkdir /mnt/AndroidClone
3. Then type the command mount /dev/sdb1 mnt/AndroidClone
4. Go to /mnt/AndroidClone/android-4.4-r5/data/system. You should see a file labeled password.key. In the terminal, type cat password.key | tr '[:upper:]' '[:lower:]' | tail -c 32
5. Copy and paste the hash string into an MD5 hash generator. Copy and paste result into new text document called echash.txt. Make sure it’s on your desktop. It should look like this: **6128754702615a2fad3707446df223e4**
6. Now go back, and type in gedit locksettings.db… this is the file containing the salt. Copy and paste the characters directly following the password salt key into the terminal after entering the command printf "%016”. Altogether, your command should look like this:

**printf "%016” 2348825145663118167**

You should end up with the hexadecimal equivalent for the salt now, it should look like this:

**2098b4067ec15b57**

Copy and paste the new salt value into the echash.txt document.

1. Inside the echash.txt file, write the values out as password:salt, it should look like this:

**6128754702615a2fad3707446df223e4:2098b4067ec15b57**

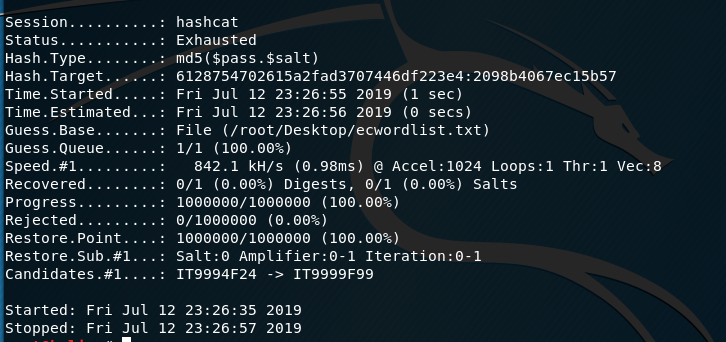
1. Now, you’re going to create a word list that includes all possible passwords for this assignment. For the sake of simplicity, we will assume it includes the uppercase letters ITF and the rest of the password is digits, totaling 9 characters long. From terminal, in the desktop directory, type:

**crunch 9 9 -t IT%%%%F%% -o ecwordlist.txt**

1. Now we are going to run hashcat to retrieve the password. From the terminal, in your home directory, type:

**Hashcat -m 10 -a 0 /root/Desktop/echash.txt /root/Desktop/ecwordlist.txt**

1. Your results should look like this:



MY NOTES

Extra Credit Assignment #1

* Enable mouse on android VM
* Password starts with IT
* Use MD5 not SHA1
* Salt in locksettings.db close to password.key

printf "%016x" 2348825145663118167 >>> end up with salt in MD5 format>>

2098b4067ec15b57

cat password.key | tr '[:upper:]' '[:lower:]' | tail -c 32

82232f22e26b101aed32f5b24a3f281 <<MD5 password hash?

82232f22e26b101aed32f5b24a3f281: 2098b4067ec15b57

Original values in hash.txt for MD5 and salt:

470DE6E1FBE88DE3E7D4AE52A196B8DDCD72D78A082232F22E26B101AED32F5B24A3F281

2348825145663118167