Learn to hack following these few steps

Introduction:

Hacking was used in the earlier days to learn information about the systems and IT generally. Thus, was not that big a problem. But in the recent times after the display of hacking in so many movies as a process to fetch confidential information it has became a big problem to the society. Thus, the concept of Ethical Hackers come into being. An Ethical hacker is a person who deliberately hacks into a system or mainframe to check the durability of the system and to find out the bugs in it. Now the Ethical hacker is a person who knows his limits and thus due to the build of this trust they earn a huge salary.

So, learning hacking is a totally different thing. It needs a very strong logic deduction capability and also the power of understanding different possibilities.

Here are some steps that will sure help you to learn to hack:

Part one of learn to hacking:

1. One needs to learn programming languages properly. Don't limit your self to any one language but then you should learn C, Python, Ruby and PHP as well. You need to follow this if you wan to learn to hack.

2. One needs to do proper research in advance before he tries to or goes for hacking. The thing is that the more one knows in advance the less surprises they get.

Part two of Hacking:

1. Use of *nix terminals for commands: The Cygwim software helps in creating the environment for windows. Nmap can be used in Linux. learn to hack using these steps.

2. Securing one's machine: This is an important thing to do. Make sure that you have safety. Look for a server that is hosting anything illegal and then try to hack it and make it yours.

3. Testing of your target: This is another important step. You need to see whether you can reach the remote computer.

4. Find out the operating system of the machine: Use of the Nmap tool for this purpose is beneficial as it can easily gather the required information for you.

5. Finding an open path or port to the system: The FTP and HTTP ports are often well protected and hardened. Other ports can be used for entering which can be brute forced.

6. Cracking the password: Cracking password is the hardest part. It needs lot of information and skill. As people nowadays are discouraged to use weak passwords. Thus, they cannot be always brute forced. Thus we need to find alternative ways. The use of rainbow tablets are the fastest way to crack passwords.

But Even then finding an alternate way to enter is preferable. One can easily learn to hack with a little bit of determination and hard-work.

Points to keep in mind:

- Users are often discouraged from using weak passwords, so brute force may take a lot of time. However, there have been major improvements in brute-force techniques.
- Most hashing algorithms are weak, and you can significantly improve the cracking speed by exploiting these weaknesses (like you can cut the MD5 algorithm in 1/4, which will give huge speed boost).
- Newer techniques use the graphics card as another processor — and it's thousands of times faster.
- You may try using Rainbow Tables for the fastest password cracking. Notice that password cracking is a good technique only if you already have the hash of password.
- Trying every possible password while logging to remote machine is not a good idea, as it's easily detected by intrusion detection systems, pollutes system logs, and may take years to complete.
- It's often much easier to find another way into a system than cracking the password.

7. Getting super user privileges: One needs proper privileges to fully interact with the system so getting administrator privileges is of paramount importance. Get to learn to hack.

Points to keep in mind:

- Most information that will be of vital interest is protected and you need a certain level of authentication to get it. To see all the files on a computer you need super-user privileges - a user account that is given the same privileges as the "root" user in Linux and BSD operating systems.
- For routers this is the "admin" account by default (unless it has been changed); for Windows, this is the Administrator account.
- Gaining access to a connection doesn't mean you can access everything. Only a super user, the administrator account, or the root account can do this.

8. Use various tricks: Often, to gain super-user status you have to use tactics such as creating a *buffer overflow*, which causes the memory to dump and that allows you to inject a code or perform a task at a higher level than you're normally authorized.

- In unix-like systems this will happen if the bugged software has setuid bit set, so the program will be executed as a different user (super-user for example).
- Only by writing or finding an insecure program that you can execute on their machine will allow you to do this.

9. Create a back door and cover your tracks: Once you have hacked a system you may want to visit again. So creating a back door is intelligent thing to do. And again you dont want to get caught so one needs to cover his tracks. Good things to do are that you dont need to add any additional users. Also dont change any passwords.

These are the basic steps for hacking. But to really learn to hack you must read and be efficient in programming languages.