BITSACM — R2

Hacking

Overview

First of all you need a good theoretical grasp on computers and a good foundation in programming knowledge. Have atleast proficiency in one programming language. Go for Python once you are done with the CP course IMO.

Now comes the fun part, learn a bit of linux commands, for this use overthewire war games (CTF). Just google for it and do your homework on how to play them and where to start . Don't follow up the solutions, break your head a bit on this.

Given you have done your CP course, you would get a firm grip on it(terminal/cmd commands) . You might feel at times you aren't actually hacking, but you need to have a base before having a good view. After having this all done, learn about NMAP, Burpsuite, Nessus, etc. and other sniffing tools. To know more about this you can google around and find such tools.

While learning about tools you need to gradually grasp concepts relating to Networks, Password cracking, Cryptography, Web security, and many more fields in hacking. Well,

this is what I know, others may give better input on hacking but I think its best if you start with Capture the flag(CTF)-(games).

Also, I didnt mention this but there are some things such as SQL injection and etc etc..but I think you will find them on your path.

Resources

1. Cybrary.it

2. **New Boston tutorials on networking**
These are just to make you comfortable with networking etc.
Then try to learn about what are wargames. And then you can learn through wargames. One such wargame is Bandit-OverTheWire.
You can go for others too. These will help you get more comfortable with Linux.

3. Security Tube is amazing place to learn something substantial.
There are many categories withing hacking also example web, crypto, pwn, forensics, steganography,etc. Learn about them and explore them.

4. Go through OWASP top 10 vulnerabilities. And learn about what they are. For example SQL injection. Learn how you can do it.

5. Learn about various common attacks like Man in the middle, DoS/DDoS, XSS, SQli(all types like boolean blind, time blind, error based).
Learn to use sqlmap for SQL in specific.

6. Then you all can start participating in CTFs. CTFtime is the website where you will find ongoing capture the flags. It is the place where you can actually practice what you learnt.

6. If you are serious about this either dual boot your laptop with Kali or dual boot with Ubuntu and use vagrant for Kali. It's also important alongside that you keep learning how to use the various tools provided by Kali Linux.

Also read:

- http://www.catb.org/esr/faqs/hacker-howto.html#teach_hack
- https://www.linkedin.com/pulse/how-prepare-oscp-certification-praveen-kumar-k-oscp/
- *"Proactive Computer Security"* on Udemy
- *"Web Application Hacker's Handbook"*
- https://github.com/stong/infosec-resources