Metasploitable hacking:

Okay I will make this very simple because so many people make setting up a lab complicated.

Set both virtual machine to host only. Now on your Kali machine open a terninal and type 'ifconfig' it will show your IP address under eth0.

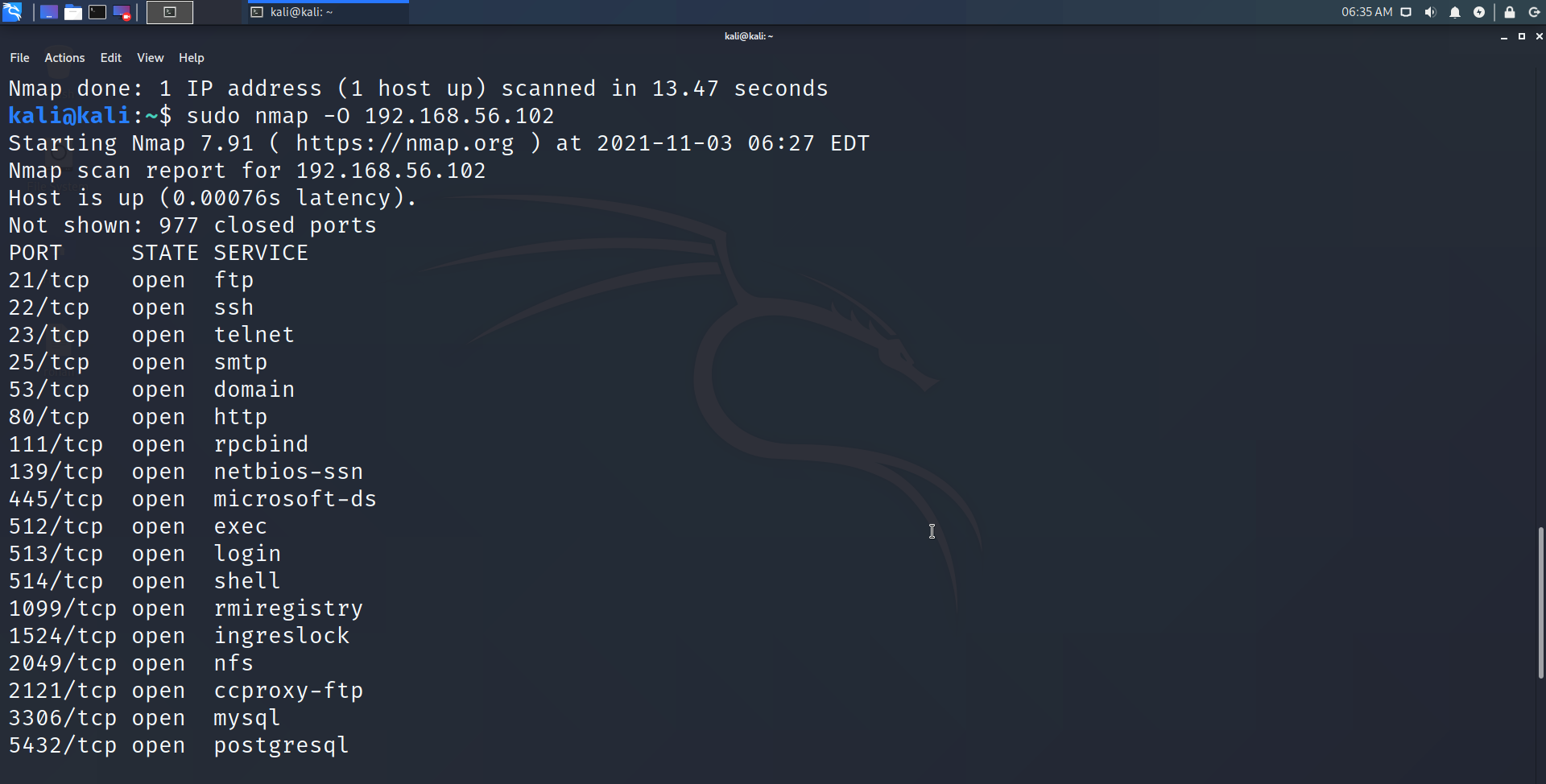
Now a couple things you can do here. Ip addresses are usually assigned logically so if you're 192.168.56.101 and you booted up your metasploitable machine second then it will probably be 192.168.56.102.

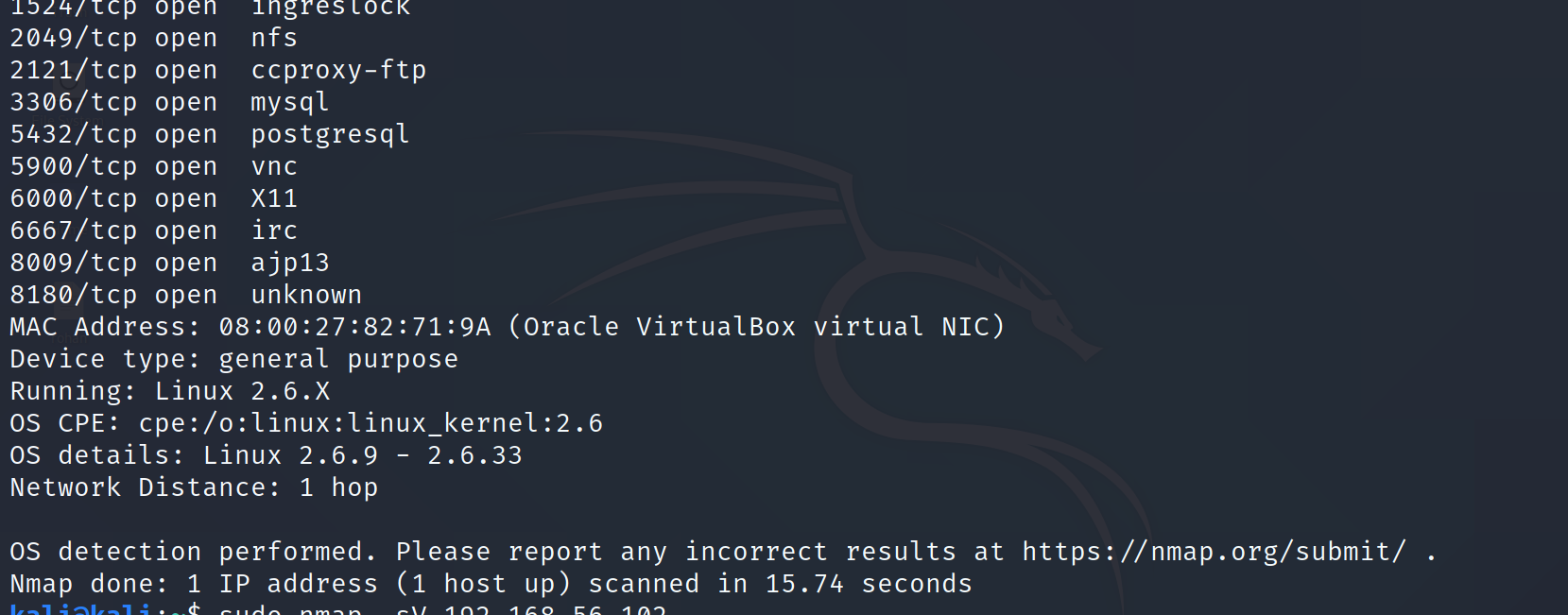
However, since you're just starting I recommend going to your metasploitable machine and logging in with msfadmin:msfadmin as username and password and typing the same ifconfig to double check.

A couple good things to know. Host only allows the VMS to only communicate with each other through your main host machine. They cannot reach outside networks which is good for sending malicious payloads through a network. You cant accidently hurt anyone. Also to double check it's working you can ping the machine using the command ping 'Ifconfig' address of other machine'

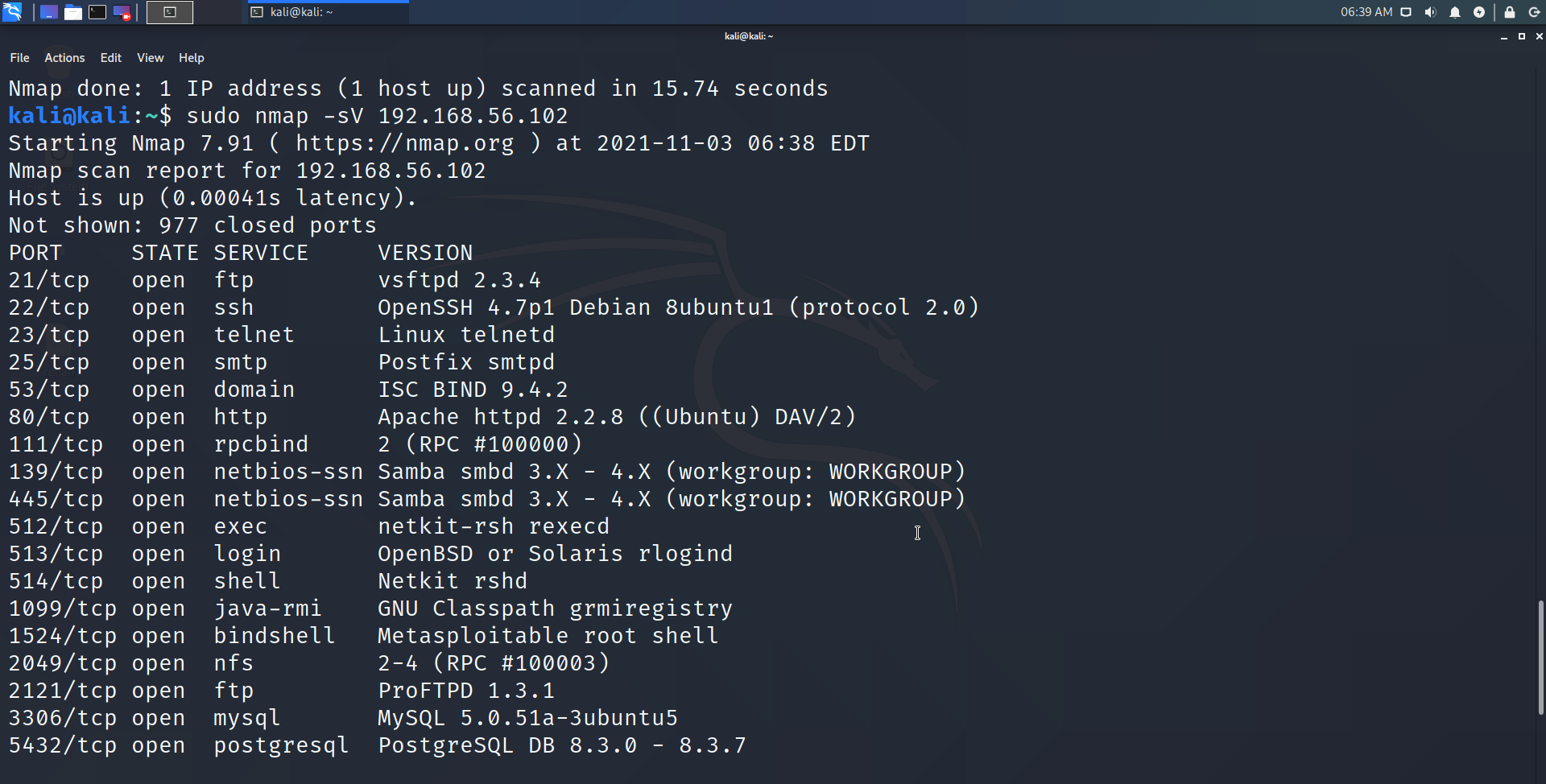
This will get you started. On future VMS you won't have access to the login right away so to find the IP address you can scan the subnet (192.168.56.0/24) or do what I said above and see if it's logically assigned to the next increment of IP address. Sometimes you'll be in a situation with a gateway router and can scan the gateway. There are numerous ways to go about this but don't worry about this right now if that doesn't make sense just continue to learn and you'll get it (:

1. Go to metasploitable and type ifconfig. See inet addr under eth0 that is the ip addr of the vulnerable os.
2. Go to kali linux and scan the ip addr using nmap,etc



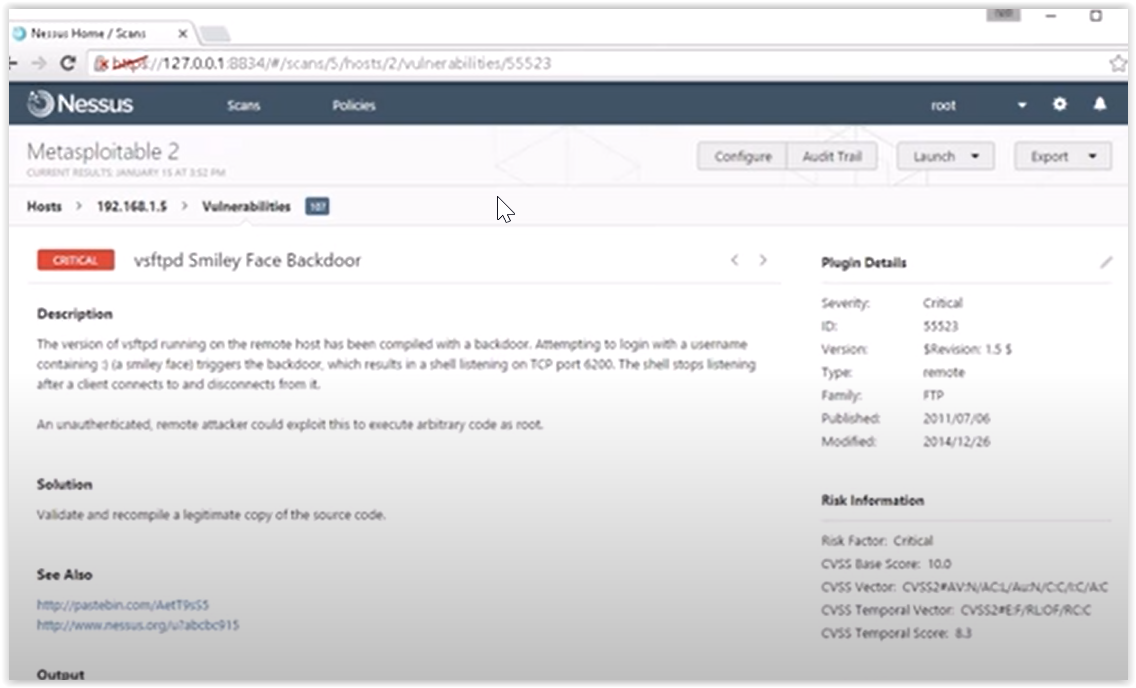


A lot of open ports meaning its vulnerable. Os details are also shown. Metasploitable runs linux



Above scan enumerates the various network services and their version which can be exploited to gain access into the system.

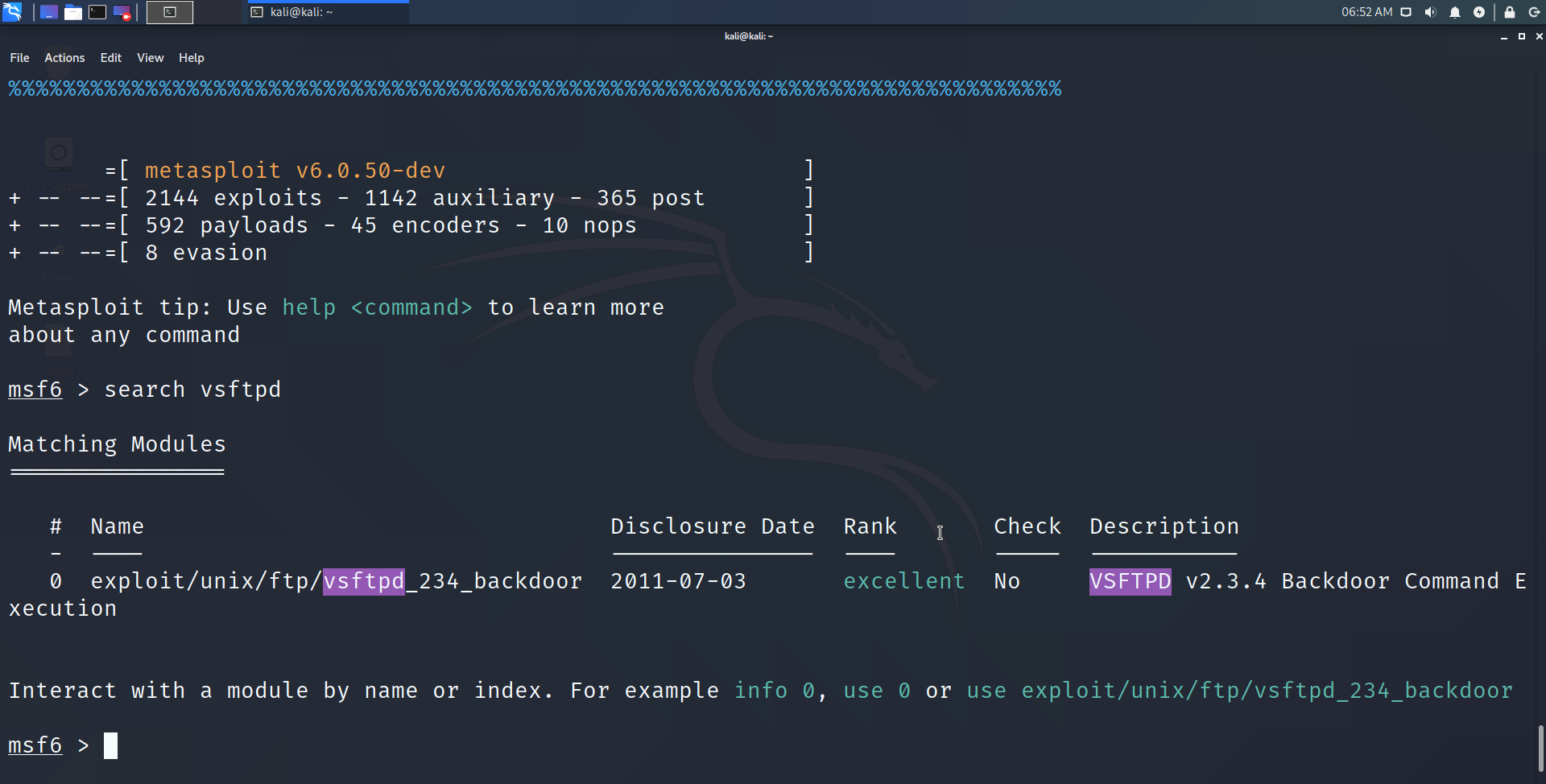
We can also open nessus website and do a more comprehensive scan than nmap. We exploit the vsftpd vuln(first one in the nmap scan).



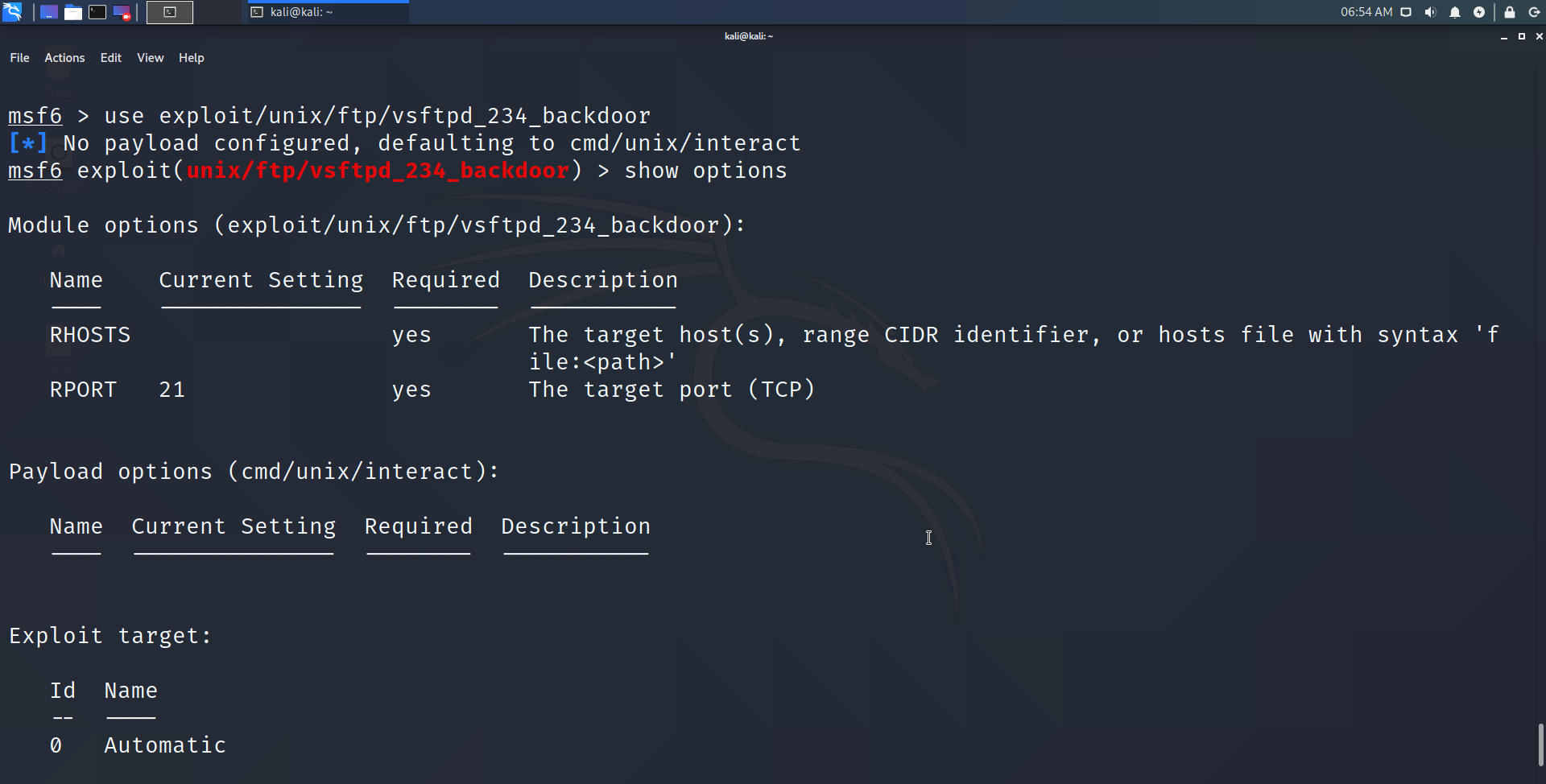
Use metasploit

Open metasploit using msfconsole

Search for the vuln as shown below

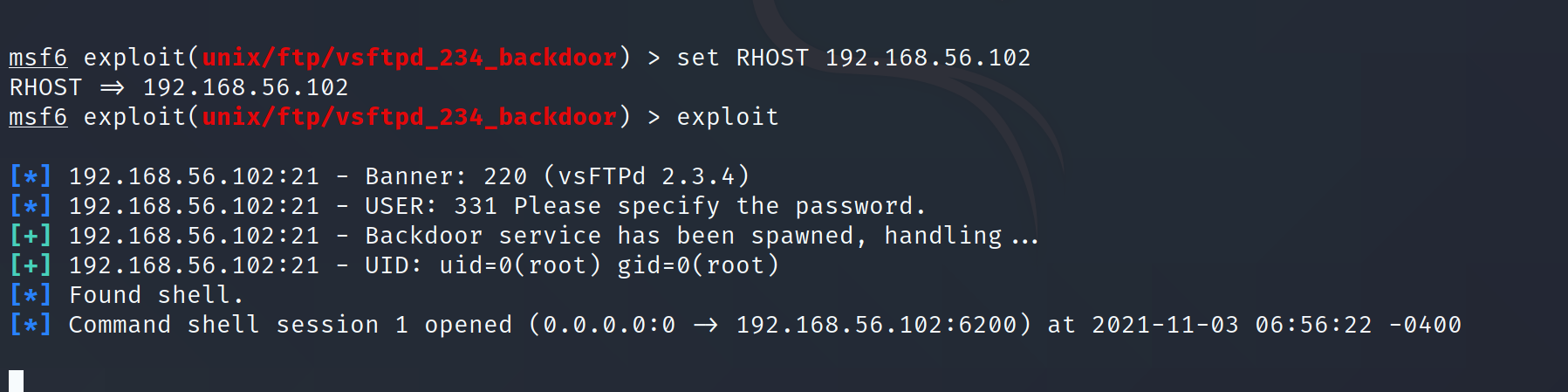


Use that vuln, and also see parameters on how to use it

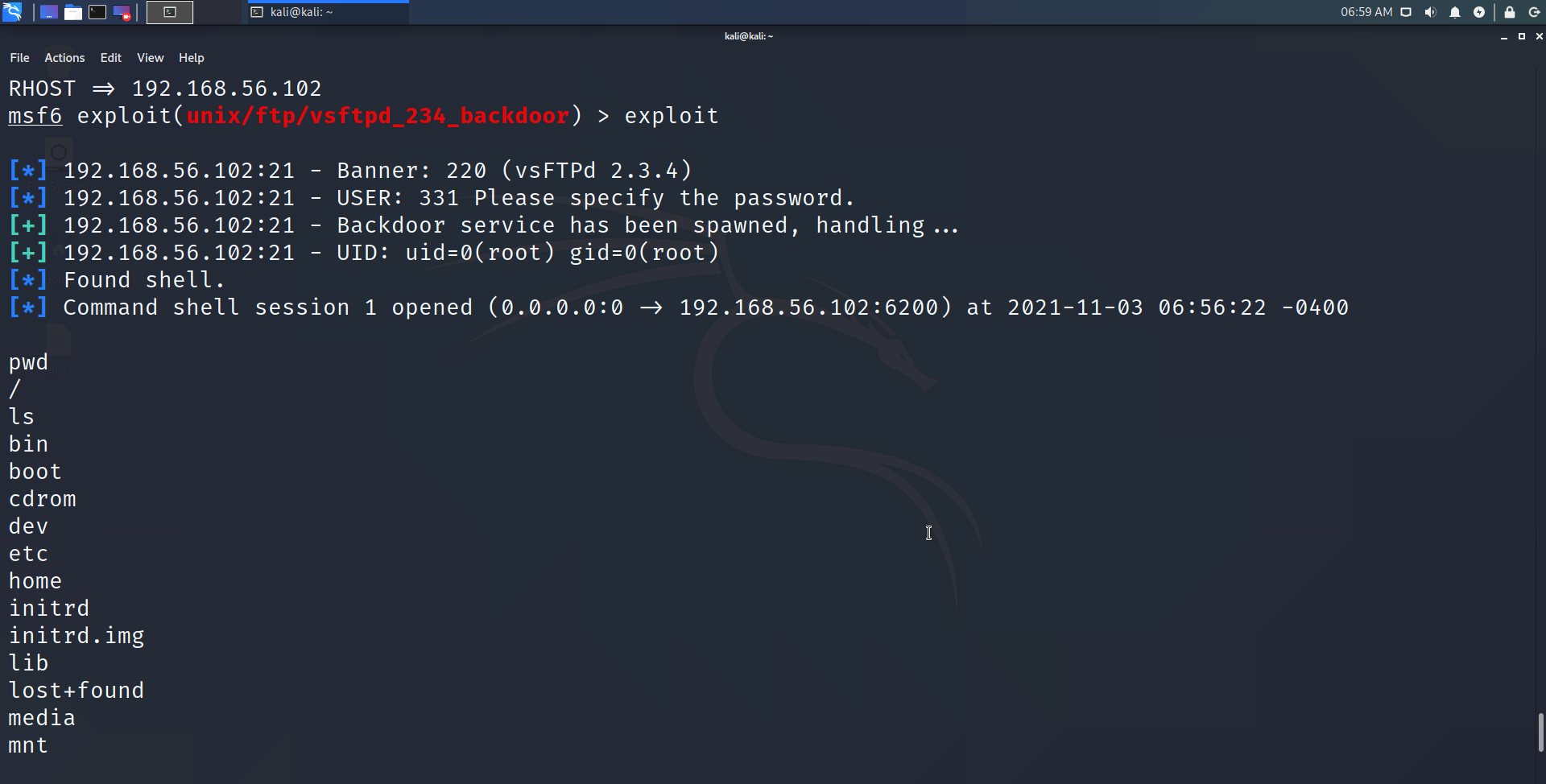


Set Rhost or the target metasploitable ip address to hack. Rport is already set at 21 for us.

And finally exploit



Now we are in the commandprompt of metasploitable from kali vm. Pwd gives the present working directory and \ signifies we are root. Ls lists all the files.



See all the users and their encrypted passwords which we can crack using tools lyk hashcat.

