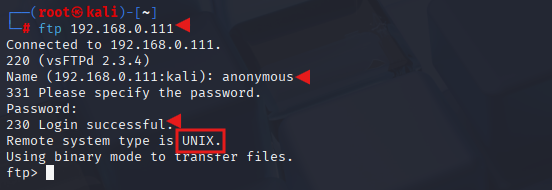
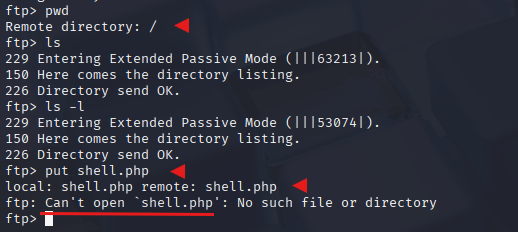
****EXPLOTATION OF FTP :**** FTP stands for File Transfer Protocol. As the name implies, it is used to share or transfer files. This service runs on port 21 by default. it has an option to enable anonymous downloads. Anonymous downloads is a type of download where anyone can download the file by logging in with the username of “anonymous” and password as anything. FTP uses clear text authentication. So if any hacker is [sniffing](https://www.hackercoolmagazine.com/beginners-guide-to-packet-sniffing/) on your LAN, he can see the username and password in plain text.

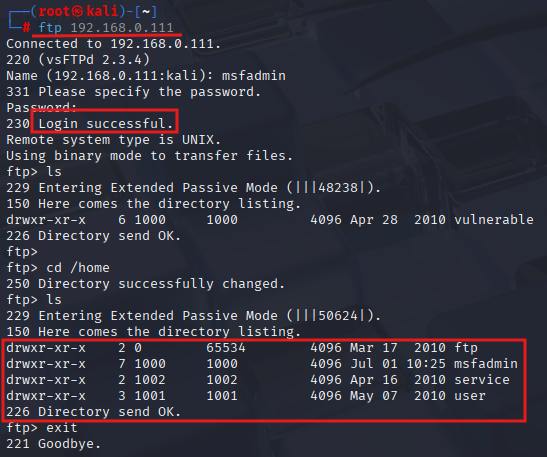


I try to login with the anonymous account (“anonymous” as both username and password) and I successfully login. Anonymous account is enabled on the target. Let’s check the permissions given to anonymous user.

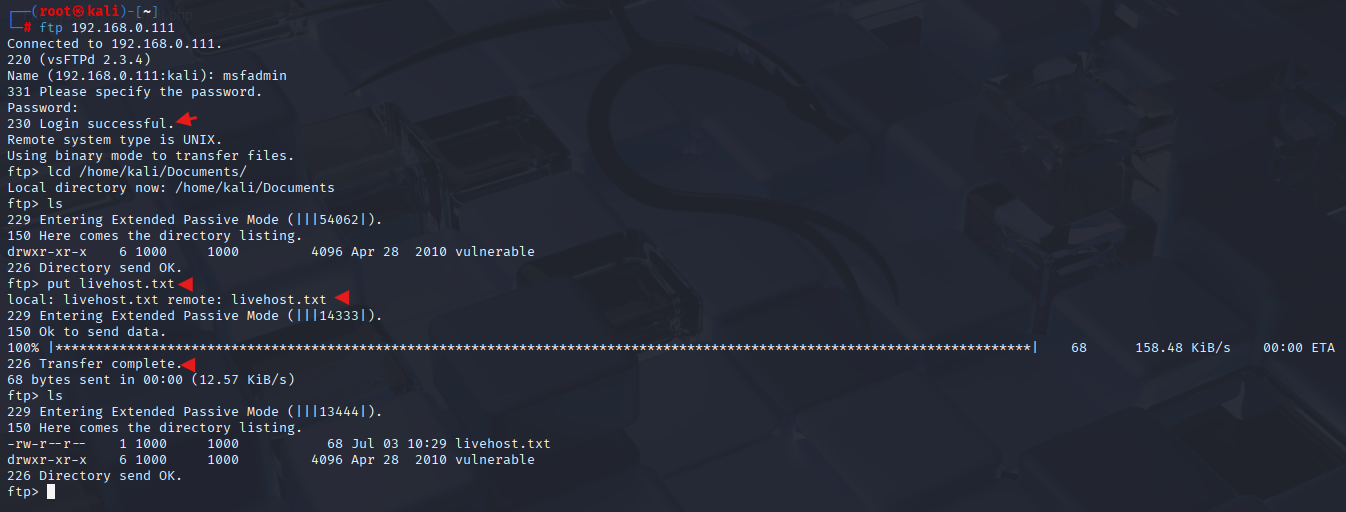


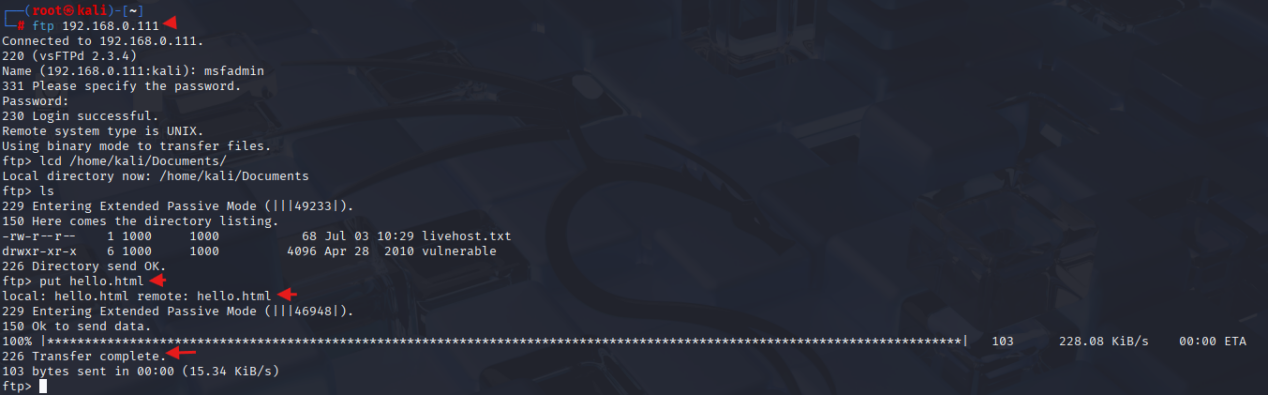
I type command “pwd” to see the current ftp directory. It’s root directory. Next I use “put” command to upload a random file to the FTP server. As you can see in the above image, file could not be created. So anonymous account has only “read” permissions. Enabling write permissions to the anonymous account may result in propagation of [malware](https://www.hackercoolmagazine.com/malware-guide-for-beginners/), pirated software etc. So anonymous account is secure in this case.

I decided to try with “msfadmin” first. The password is also “msfadmin” for user msfadmin. Login successful. I first checked the contents of the ftp directory. It seems this account has admin rights on the FTP server.



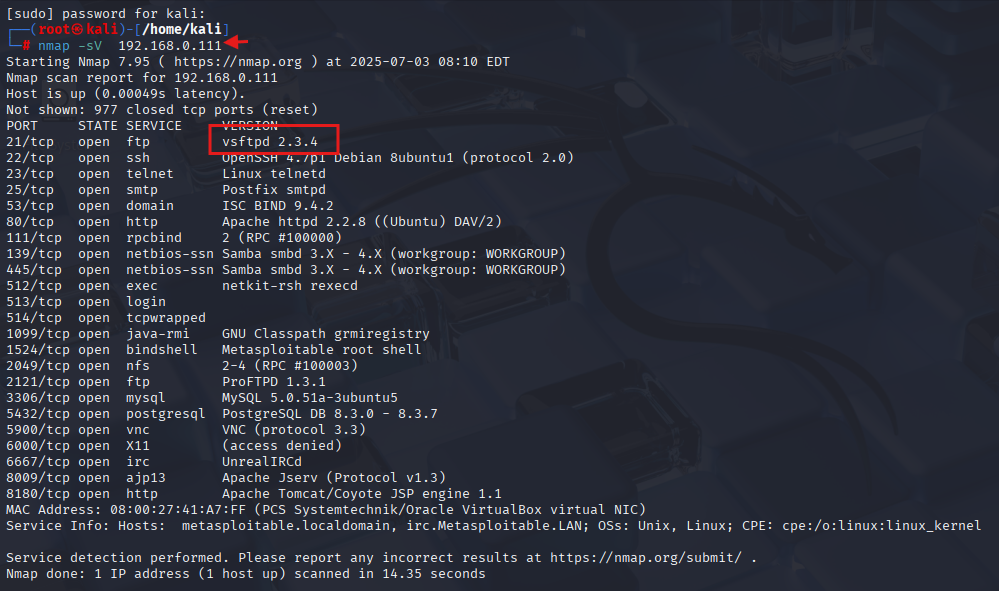
I once again try to upload the “hello.html” “livehost.txt” into the FTP directory. This time it’s successful.





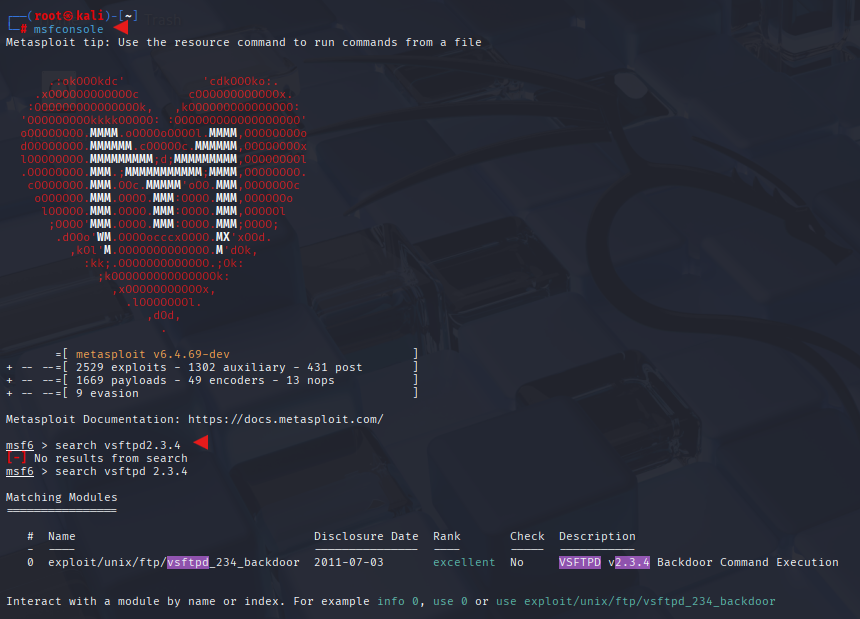
Now I can upload any malicious file to the server and can use it for any nefarious purpose. or propagation.

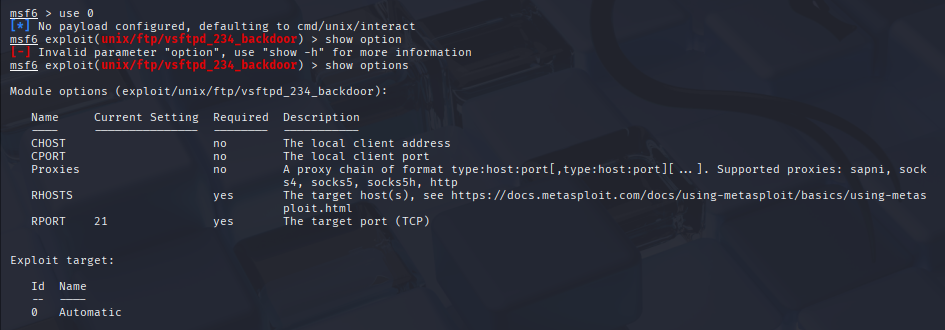
**VSFTPD 2.3.4 :** While performing verbose scan with [NMap](https://www.hackercoolmagazine.com/complete-guide-to-nmap-port-scanner/), the target has displayed banners of so many services running on the target system.



The FTP server running on port 21 is “vsftpd 2.3.4”. Vsftpd stands for very secure FTP,found that the version installed on Metasploitable 2 (i.e 2.3.4) has a [backdoor](https://www.hackercoolmagazine.com/beginners-guide-to-backdoor/) installed inside it. This backdoor was introduced into vsftpd server’s official download archive. This malicious version of vsftpd was available on the master site for download between June 30th 2011 and July 1st 2011. So our target might have installed the malicious version.

So I start Metasploit and search for the exploit. Using command “msfconsole”





I loaded the module and checked the options it needs using “show options” command. The only option required is the IP address of our target to be specified in the RHOST option. I [set](https://www.hackercoolmagazine.com/social-engineering-toolkit-set-beginners-guide/) the RHOST option and execute the exploit using the “run” command. successfully got a [shell](https://www.hackercoolmagazine.com/beginners-guide-to-shells-in-hacking/) on the target system. As shown in snapshot below.



we have shell access, we can perform all tasks which we perform from the terminal of a Linux system. We can even shutdown the remote system but keep in mind that you will lose your access to the system.

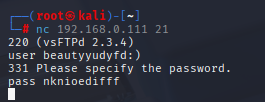
**Manually Running VSFTPD :**  Using netcat or nc command to allow us to connect to establish a TCP or UDP connection to any open port on a remote server. As shown in the snapshot. We can use any username and password but the key part is “**:)”** If you don’t use this the exploit doesn’t work

Syntax :

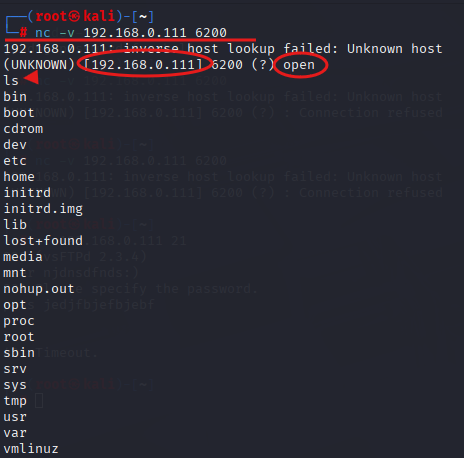
user<string>:)

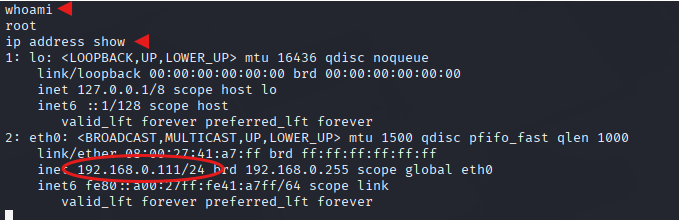
pass<string>

We won’t be finding any feedback or cautions seems like it didn’t done anything but it actually opened a shell on port number 6200. when we used the **“:)”** in the username.



Now we get an access for port number 6200. In the command we are using tag “-v” to know weather the connection is successfully established or not if we don’t use “-v’ we need to run the command to see weather the connection established or not. -v makes things easier here.





We are inside the metasploitable 2 as we can see the snapshot, we entered into it using backdoor.