Ethical Hacking Exercise

*A report on penetration testing in Metasploitable -3*

* *Prof. Sambuddho*

My first experience to computer security subject. In this exercise we were given metasploitable-3 as a vulnerable machine, in which we need to do penetration testing. Following is a report on how I explored this exercise.

1. Setup:

* I installed virtual box for installing my virtual machines - its a tool that helps virtualizing multiples computers inside one. Multiple machines can share the same hardware resources from host and run independently inside a virtual box.
* Next, I installed Kali Linux into my virtual machine, a common distro of Linux used specifically for penetration testing.
* Also imported the given vunerable machine, into it.
* And, the most important thing, changed the machines network settings to Bridge adapter, internet access was easy using NAT however for exact IP as per my PC, connected the VMs via bridge adapter. Internet connection was not accessible when used in college’s wifi, so had to do in mobile hotspot.

# A shortcut:

We were not given any default username and password to access the VM, but upon a little research found out a link where it should how we could reset root password of a Linux based VM. [Link](https://okeanos.grnet.gr/support/faq/cyclades-what-is-the-username-and-password-of-my-vm/)

What I did was went into the GRUB menu , booted the VM in recovery mode, typed in

-> mount -n -o remount,rw /

-> passwd

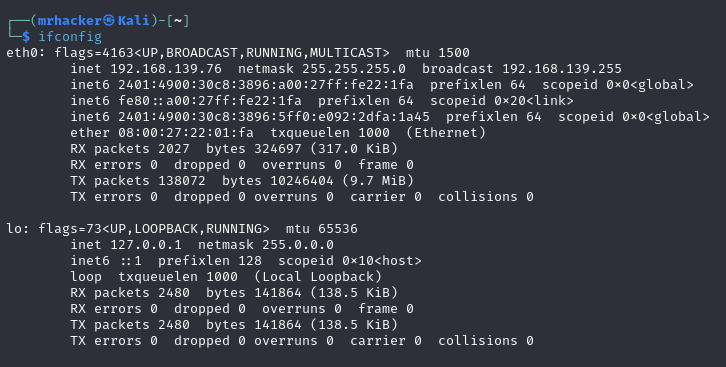
And thus I was able to reset the password. This is not what we were expected to do, still

just showing it here, as it was the first thing we came into.

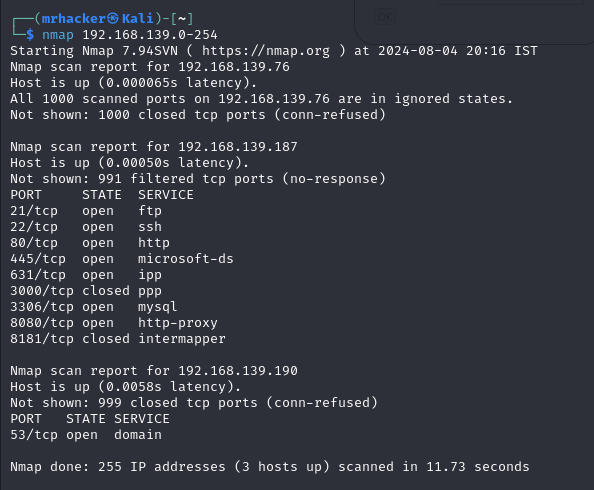
1. Information Gathering / Reconnaissance:

Trying to find any information that can help us get access into the system. First and foremost thing was to find the IP address of the VM, as thats the only way we can actively gather information about the VM.

For that, inside our Kali Linux machine, we first used *‘ ifconfig’* to find our KaliLinux machines IP address and then using the ‘*nmap’* command looked, scanned all the ports, network interfaces connected. This was to discover the vulnerable machines IP as it could utmost be different from host in the 4th octet of IP address..



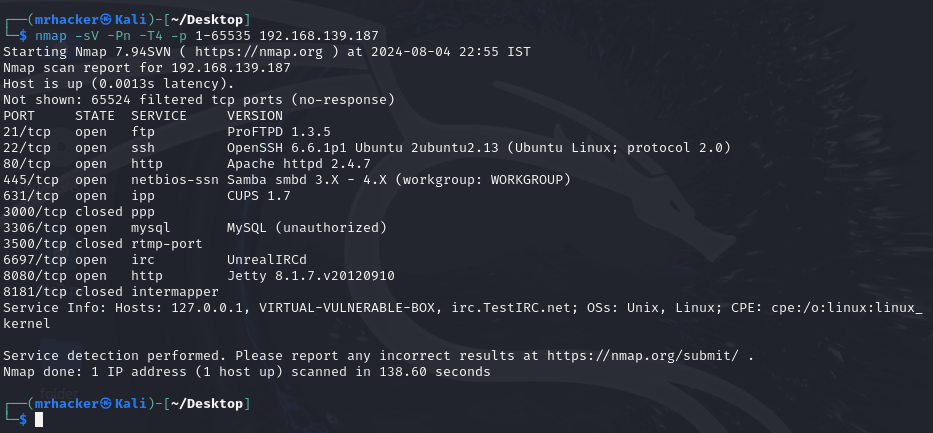
IP of my host machine : 192.168.139.76



It was very clear that 192.168.139.187 was my target VM’s IP address. I got to know identifying Mac address was how my friends discovered however, this is how I did. Only when the VM was open was this …187 IP visible and it had a lot of known vulnerabilities.

Okay, now I had the IP address of my VM, and know I needed to know more about all the technologies it was using so as to find any vulnerabilities, openings to exploit and gain access.

So, I ran the nmap command on the target machine’s IP. The nmap command has a lot of arguments, got to know via search into the internet.



I investigated all those open ports, the technologies used and searched online if they had some known vulnerabilities. And yes, there were, almost all techs you can see in the version column have vulnerabilities, now my task was to see if I can gain access exploiting them.

1. Playing around with ports, surfing to understand about the vulnerabilities:

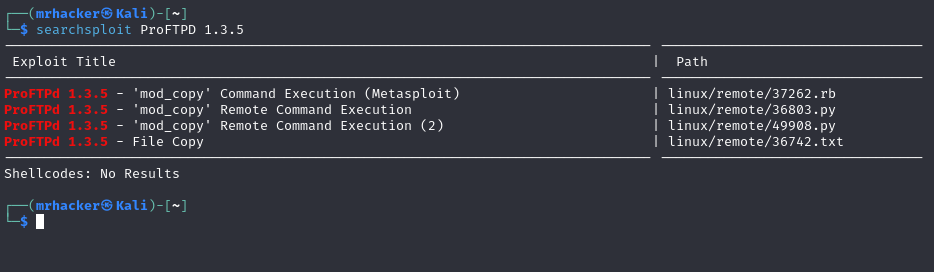
I ran checks on most of the technologies used, looking if they have known vulnerabilities, got to know their is a website named *‘Exploit-DB’,* which is technically an archive of known public exploits and proof-of-concepts for those vulnerabilities.

Some of the vulnerabilities I could encounter on Internet were :

1. Apache 2.4.7 ‘ s -> Scoreboard handling race condition
2. …
3. …
4. …

After a little research, I got to know there is a command named *‘ Searchsploit ’ ->* a command-line tool that allows users to search through the Exploit Database (ExploitDB) repository directly from their terminal. So, the surfing thing was not much of use.

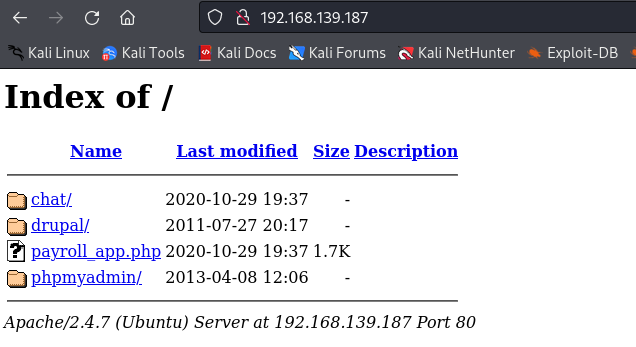
I ran this searchsploit command on some of the technologies used in open ports of VM into the terminal and was able to identify a few vulnerabilities in each, one of such search is below:



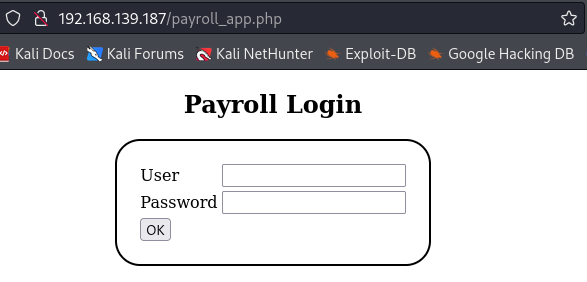
1. The Exploiting Part :

(4. A) SQL Injection

The first thing I did was typed the IP of target machine into a browser - got to know this gives some info - and it actually did, I could see a website:

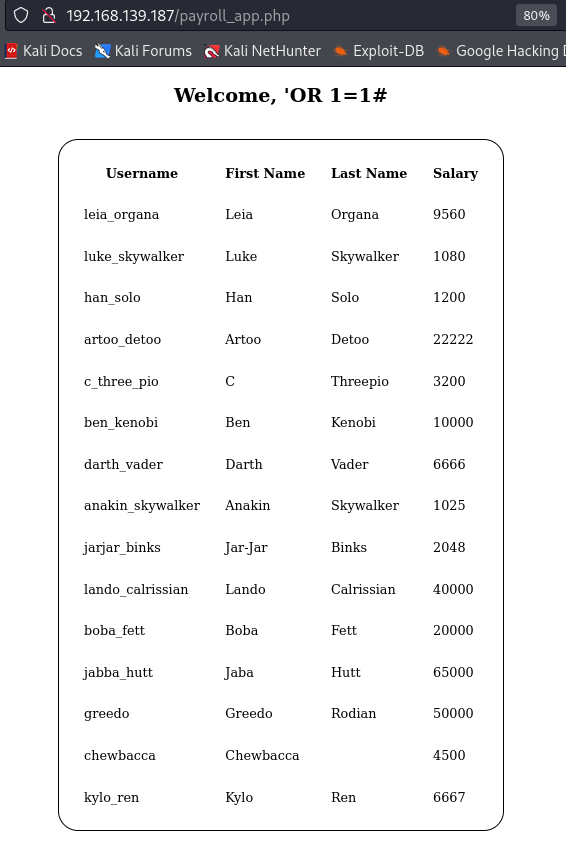


The payroll\_app.php looked a little fishy, clicked into it, and so in others, but found something interesting here.



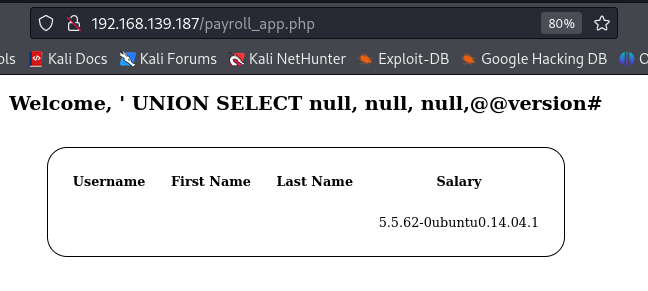
During the nmap search, there was mentioning of MySQL as well, since the version was hidden, I couldnt look into it more, but this opened up a lot, I knew a little about the SQL injection attack, and open researching more found a few codes, to try and see if we could get something out of the database.

1. Typed ‘OR 1=1# into the username field -> and hurray I could login without password.



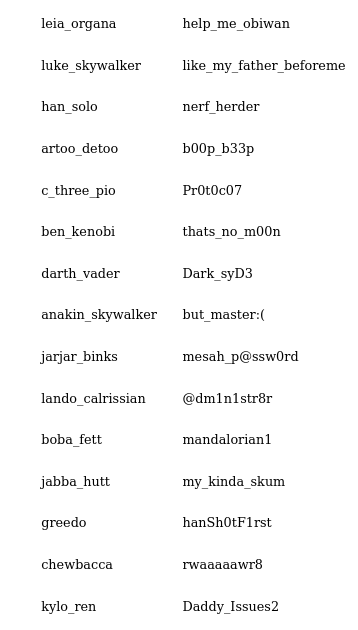
1. Next query: ' UNION SELECT null, null, null,@@version#

-> to get the version name of MYSQL : 5.5.62-0ubuntu0.14.04.1

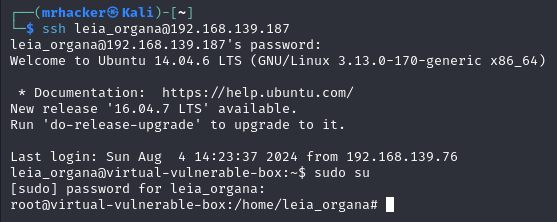


1. And the most important one : ' OR 1=1 UNION SELECT null,null,username,password FROM users#

-> this showed up the login : username and password. How I got to know they were passwords : we tried logging via them and it worked.

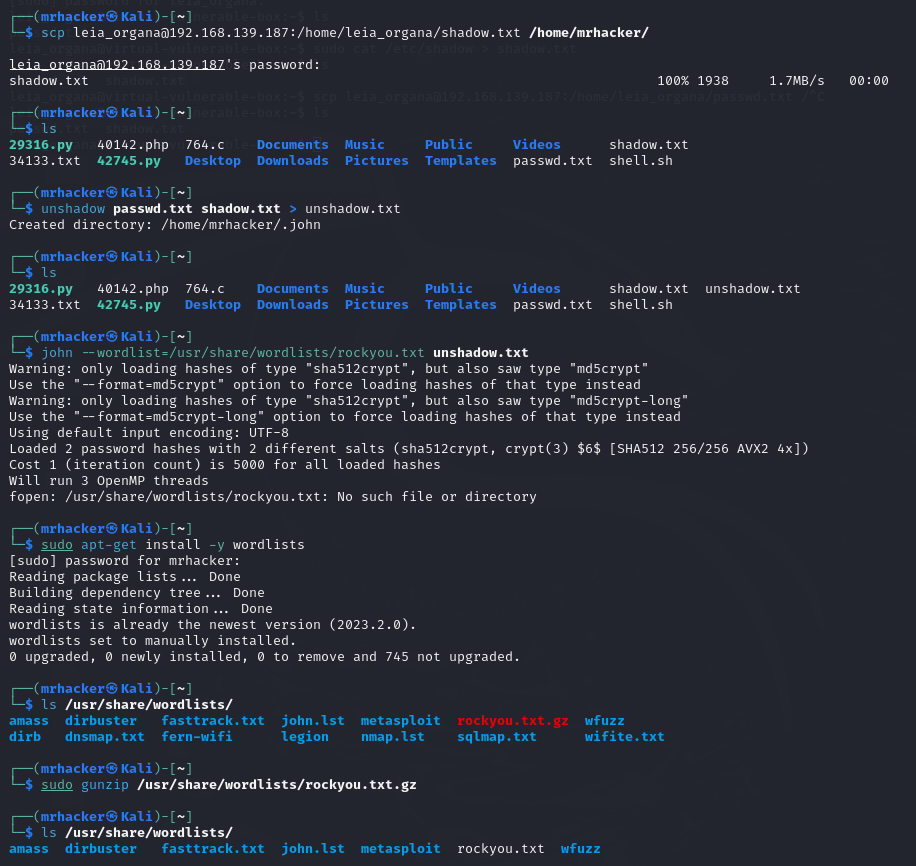
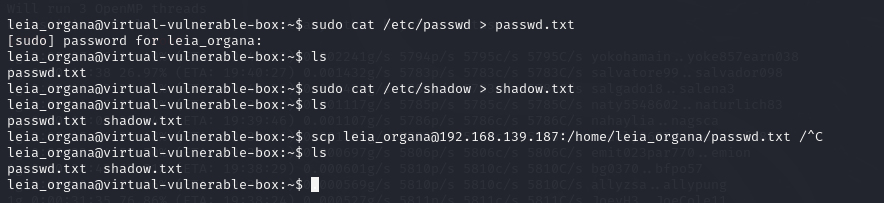


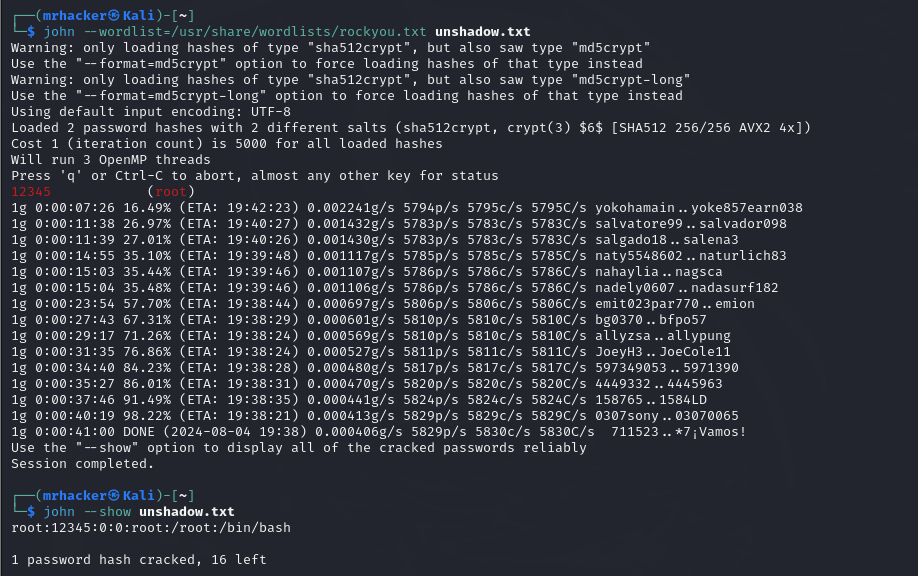
Tried to access, the VM via a username, and found it was an admin one: so I successfully gotroot access to the vulnerable machine. These are the 15 username and passwords.



In the assignment it was written to find one non root password: don’t know if it counts on these 15 or not, but I went on trying to find them. I ran the following commands to get the password files, with help of ChatGpt and browsing over different links, got to know that we needed to make a file which John The Ripper Tool could bruteforce into to crack the hash passwords.

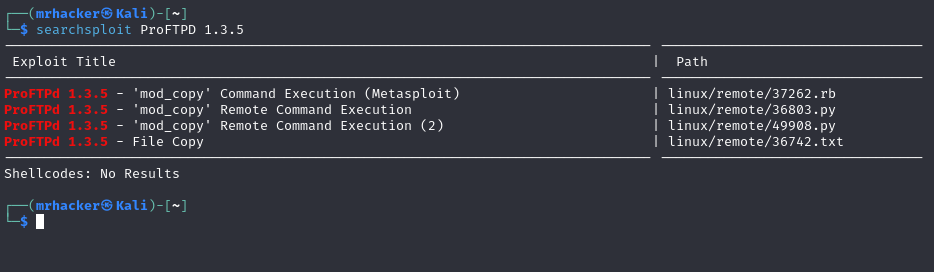
Downloaded and shared to the host machine to run the bruteforce:

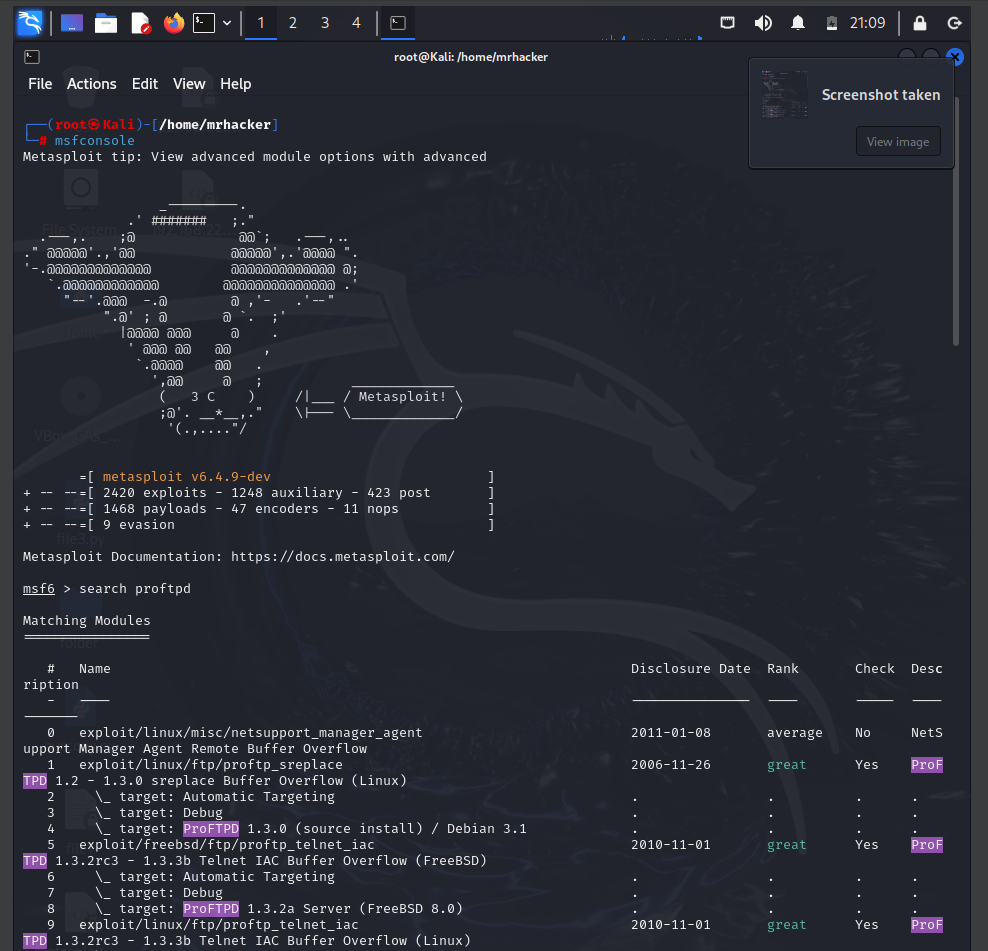


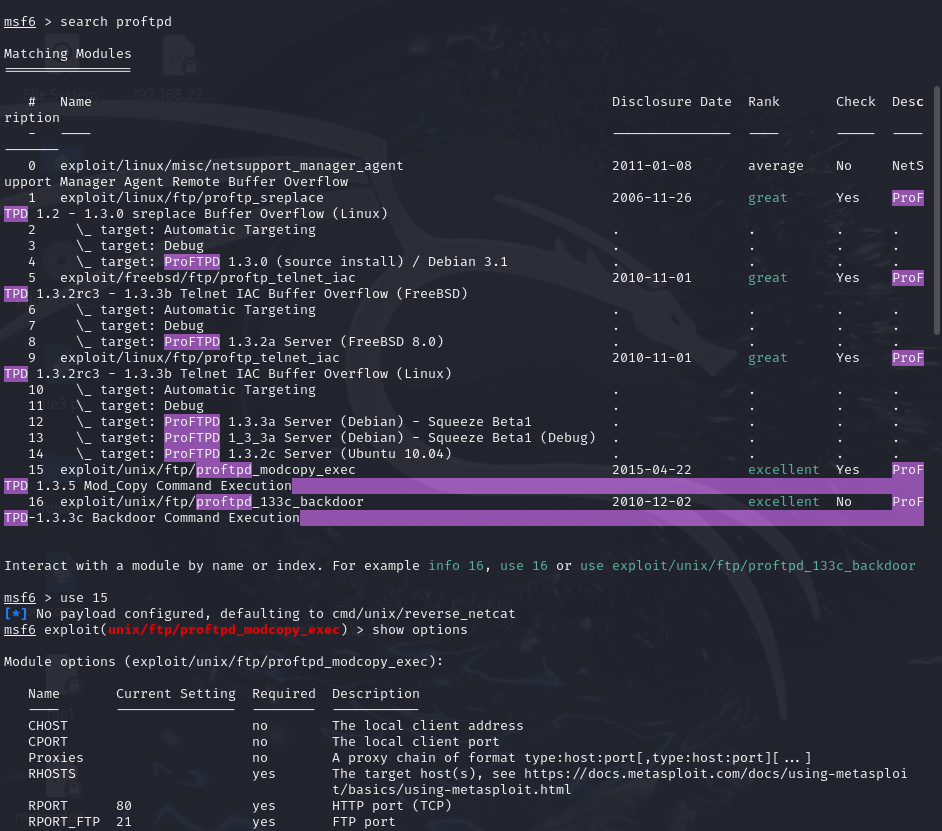


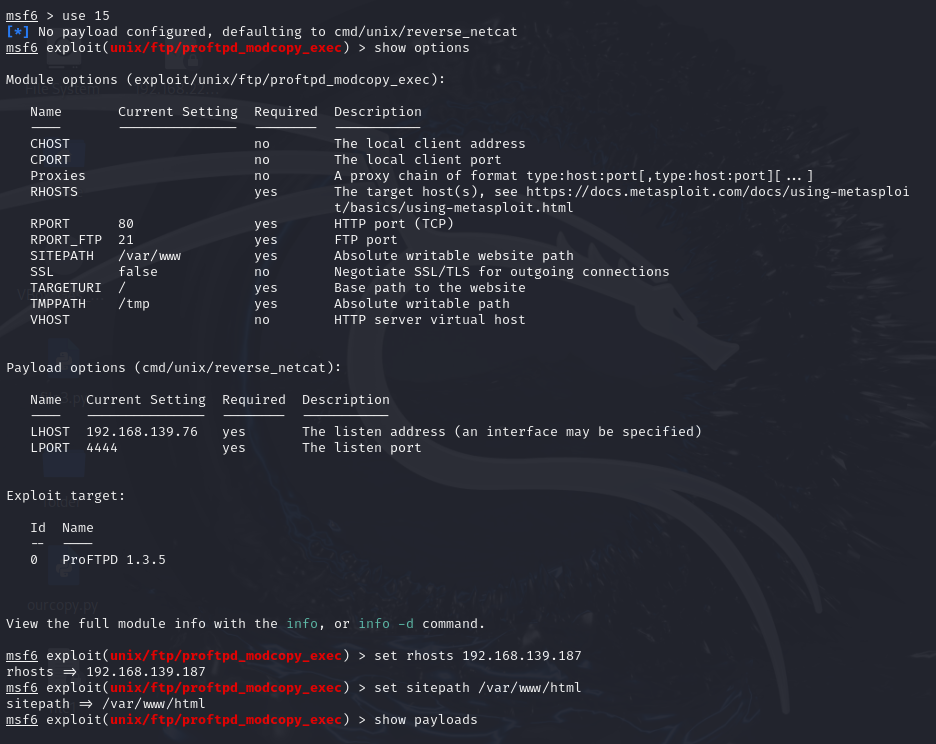
Well, can’t say I got success in it, but learnt how to use John The Ripper as a password cracking tool.

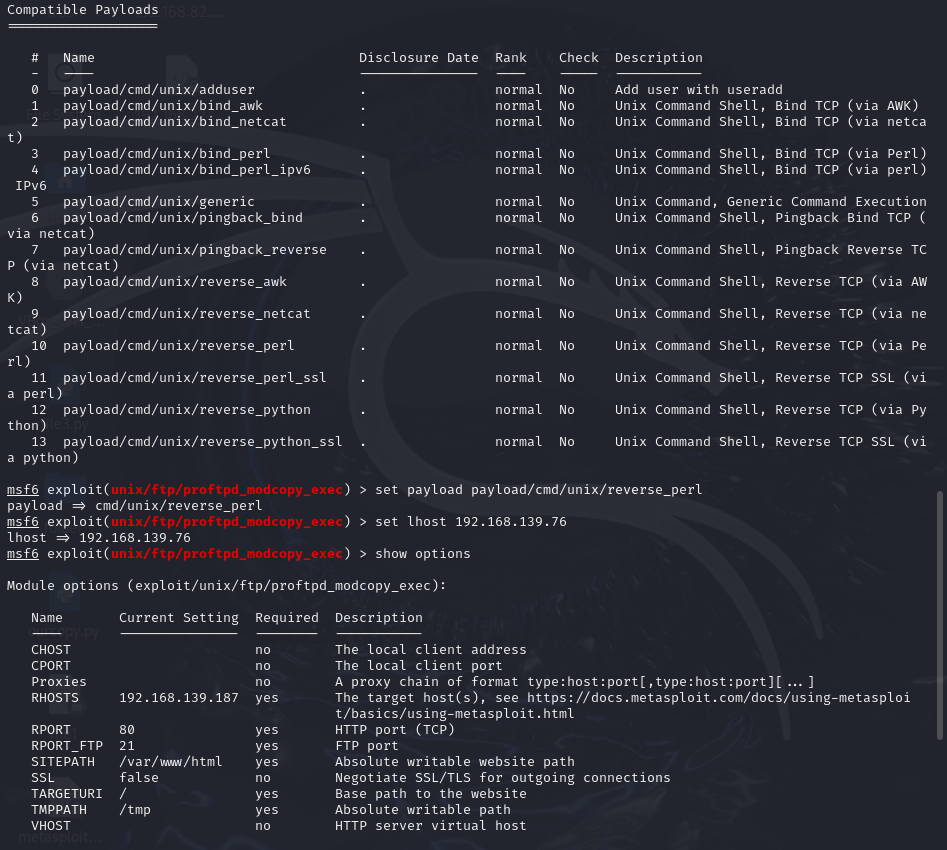
(4.B) Exploiting the FTPD service:

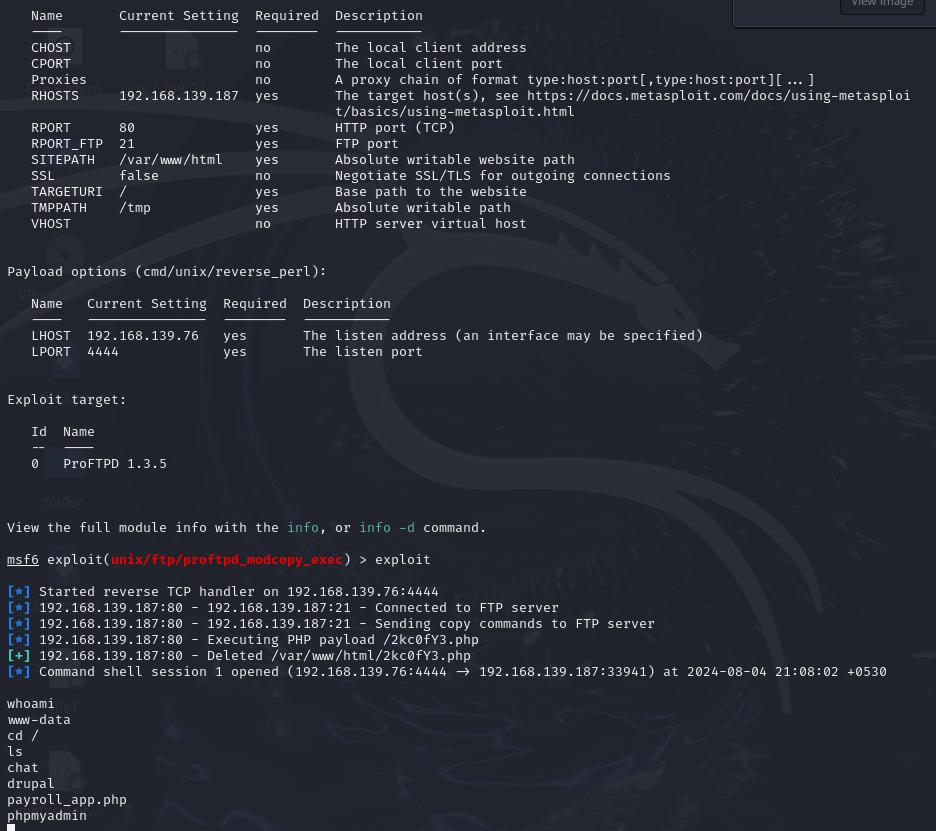






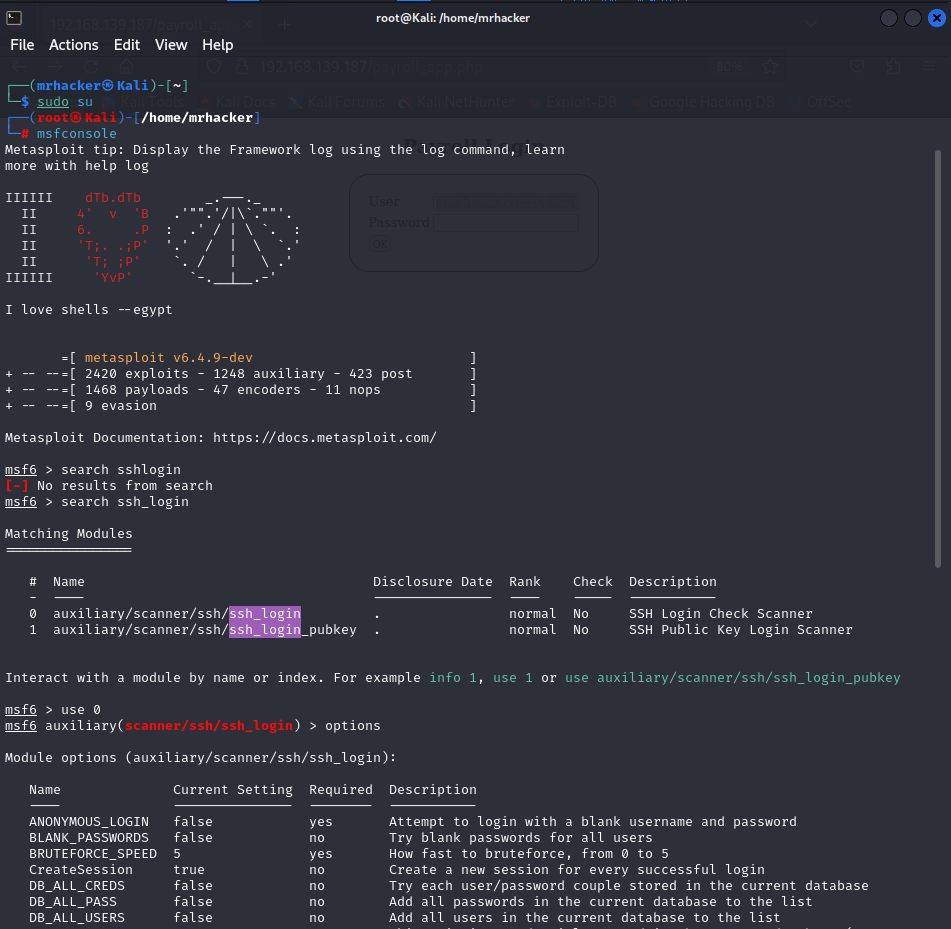


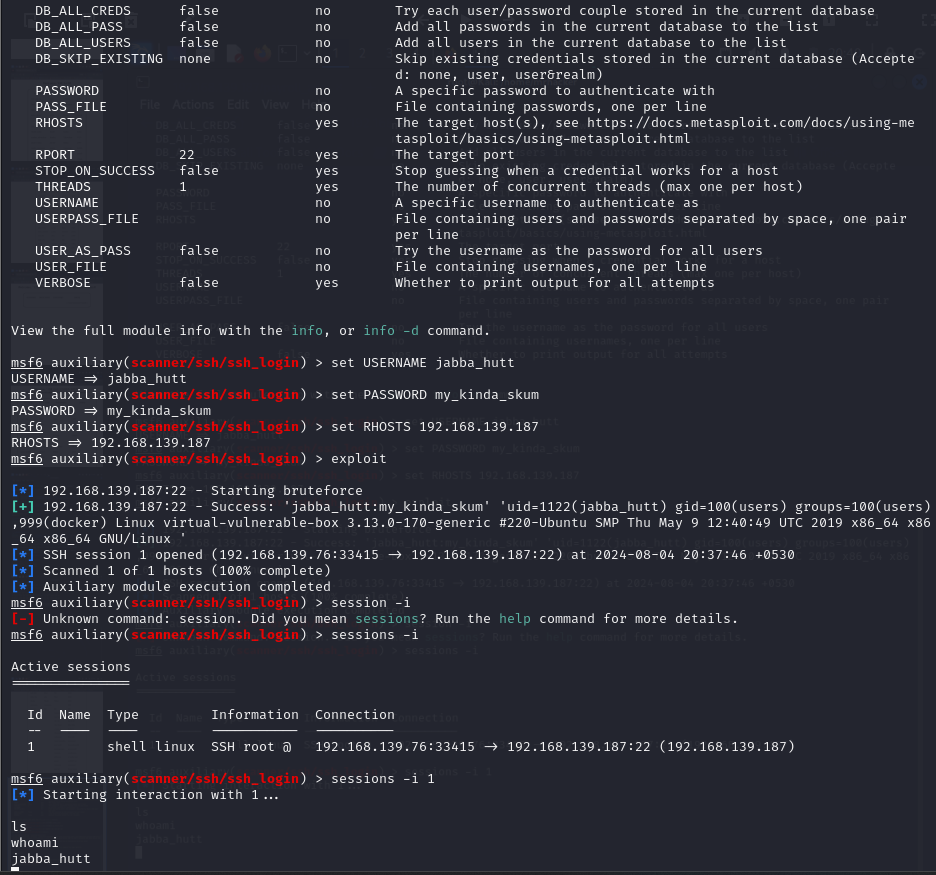




Thus, using all these commands, I could exploit the FTP port and get access to the www-data.

(4.C) Another exploit of the SSH Login :





This was how, I could exploit the SSH Login to login into any user, and access the virtual machine as if the user was, something like remote.

Could do only this much, this exercise demanded time, atleast for beginners like us, who are learning from scratch. To tell the truth, the online course on Coursera was not a lot helpful, as it had a lot theory than what was needed here. Took help from seniors, friends, ChatGpt and endlessly searched into the internet for doing whatever I mentioned into the report.

Thanks,

Prajil Bhagat.