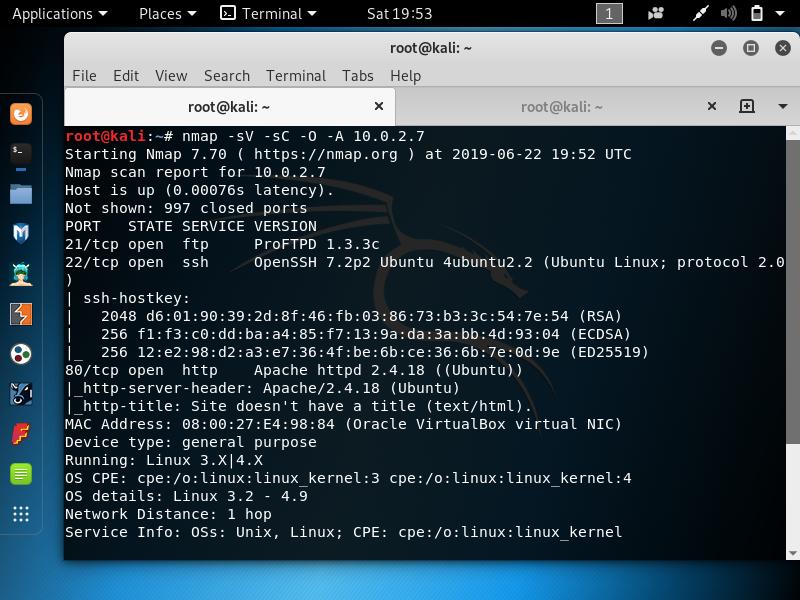
## # enumeration

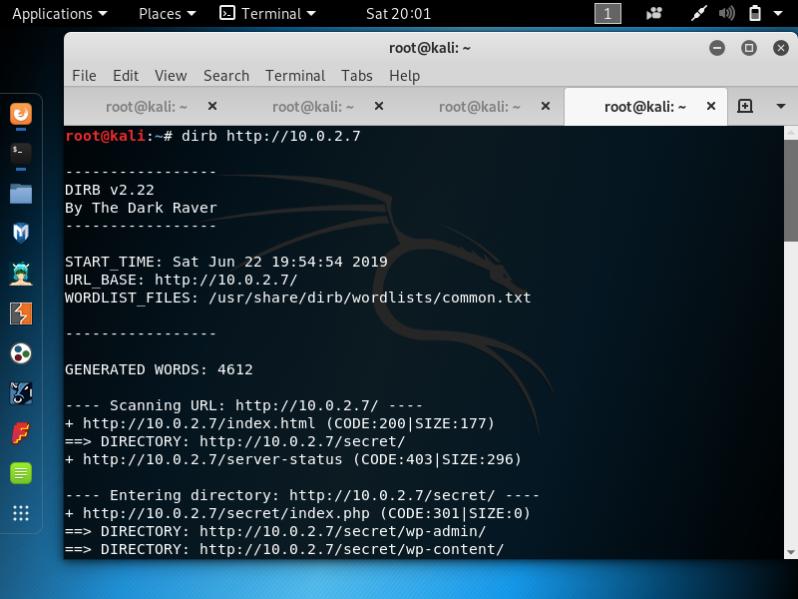
# I used Nmap for enumeration and scanning.

# nmap -sV -sC -O -A 10.0.2.7

# These options are used for aggressive scan and os fingerprinting, results are given below:

#

Running dirb results are given below:



# there are important directories that , I found out using dirb ,it is very useful for finding hidden sub-directories and in any website.

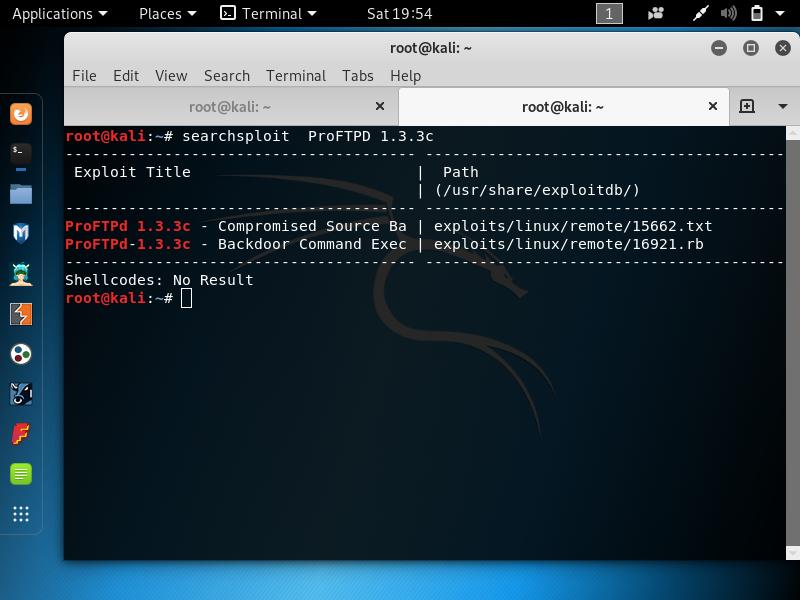
# using dirb found the directory, <http://10.0.2.7/secret> this is a basic wordpress html page.

# Results are given below.



# I saw port 21 is open that is running ftp service, I searched for the exploits using searchsploit.

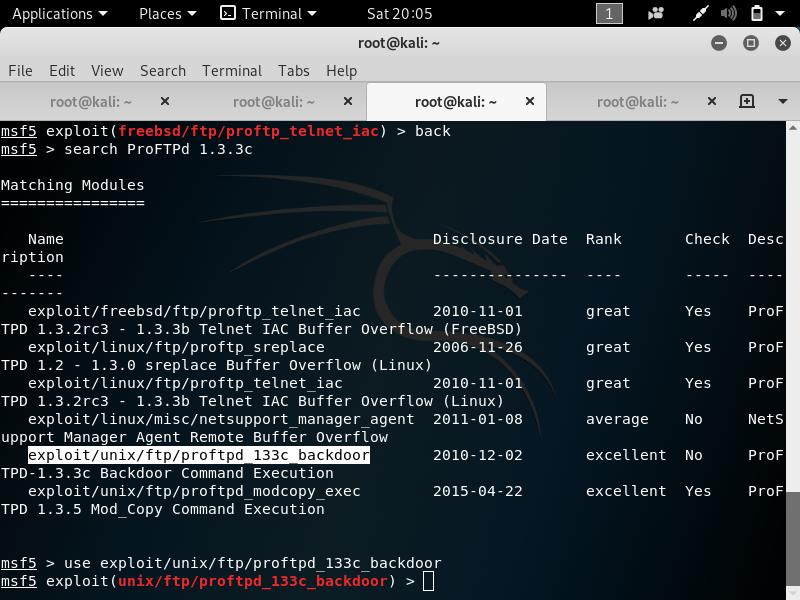
# Results for the version running on port 21 for ftp service:



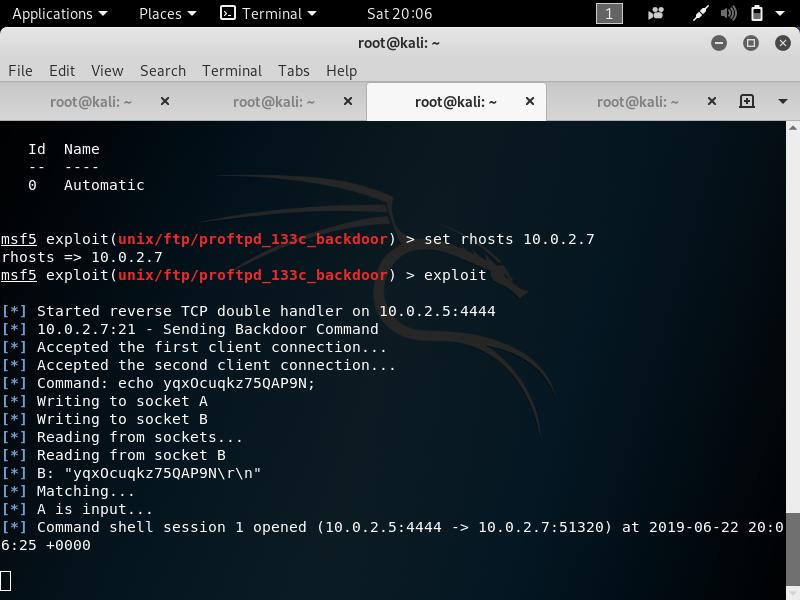
## # Exploitation

# Here I used metasploit to exploit the vulnerability on port 21.

# Results are given below:

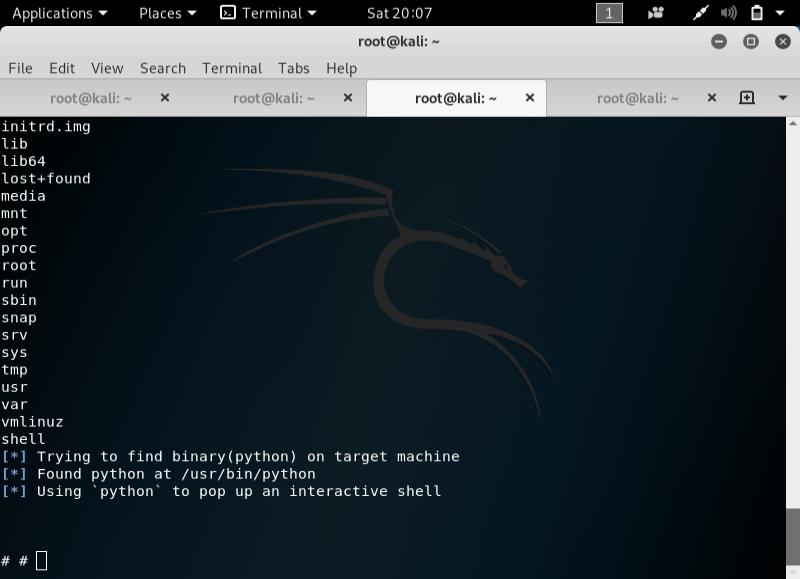


# using Metasploit I gained the shell.



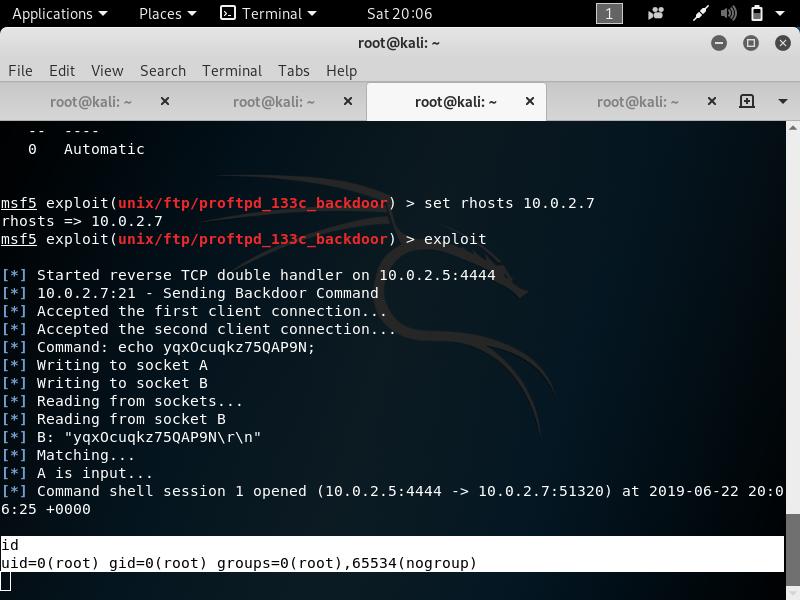
## # privelage esclation

# we just need to gain the root access in this machine there is no flag as such in this vulnhub machine.



# Here we gained the root access:

# Results are shown below:



#This is a beginner level pentesting vm from Vulnhub, As I am a beginner I chose to start with the basic one to get an idea.