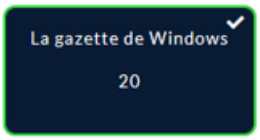

La donnée de charge utile est tracée dans un fichier : flag.ps1. Il s'agit de la lecture de la chaîne $s (cette chaîne apparait dans le log des événements et correspond manifestement au contenu du flag):

```
$l = 0x46, 0x42, 0x51, 0x40, 0x7F, 0x3C, 0x3E, 0x64, 0x31, 0x31, 0x6E, 0x32, 0x34, 0x68, 0x3B, 0x6E, 0x25, 0x25,
0x24, 0x77, 0x77, 0x73, 0x20, 0x75, 0x29, 0x7C, 0x7B, 0x2D, 0x79, 0x29, 0x29, 0x29, 0x10, 0x13, 0x1B, 0x14, 0x16,
0x40, 0x47, 0x16, 0x4B, 0x4C, 0x13, 0x4A, 0x48, 0x1A, 0x1C, 0x19, 0x2, 0x5, 0x4, 0x7, 0x2, 0x5, 0x2, 0x0, 0xD, 0xA,
0x59, 0xF, 0x5A, 0xA, 0x7, 0x5D, 0x73, 0x20, 0x20, 0x27, 0x77, 0x38, 0x4B, 0x4D
$s = ""
for ($i = 0; $i -lt 72; $i++) {
    $s += [char]([int]$l[$i] -bxor $i)
}
echo $s
```

Il s'agit d'autoriser auparavant les opérations par l'interface shell. L'exécution du script donne l'affichage du flag.

if((Get-ExecutionPolicy) -ne 'AllSigned') { Set-ExecutionPolicy -Scope Process Bypass };

```
PS C:\Users\P51S\Documents\FCSC2023\INTRO\LagazettedeWindows> if((Get-ExecutionPolicy ) -ne 'AllSigned') { Set-Execution
Policy -Scope Process Bypass };
PS C:\Users\P51S\Documents\FCSC2023\INTRO\LagazettedeWindows> ./flag.ps1
FCSC{98c98d98e5a546dcf6b1ea6e47602972ea1ce9ad7262464604753c4f79b3abd3}

PS C:\Users\P51S\Documents\FCSC2023\INTRO\LagazettedeWindows>
```

FCSC{98c98d98e5a546dcf6b1ea6e47602972ea1ce9ad7262464604753c4f79b3abd3}