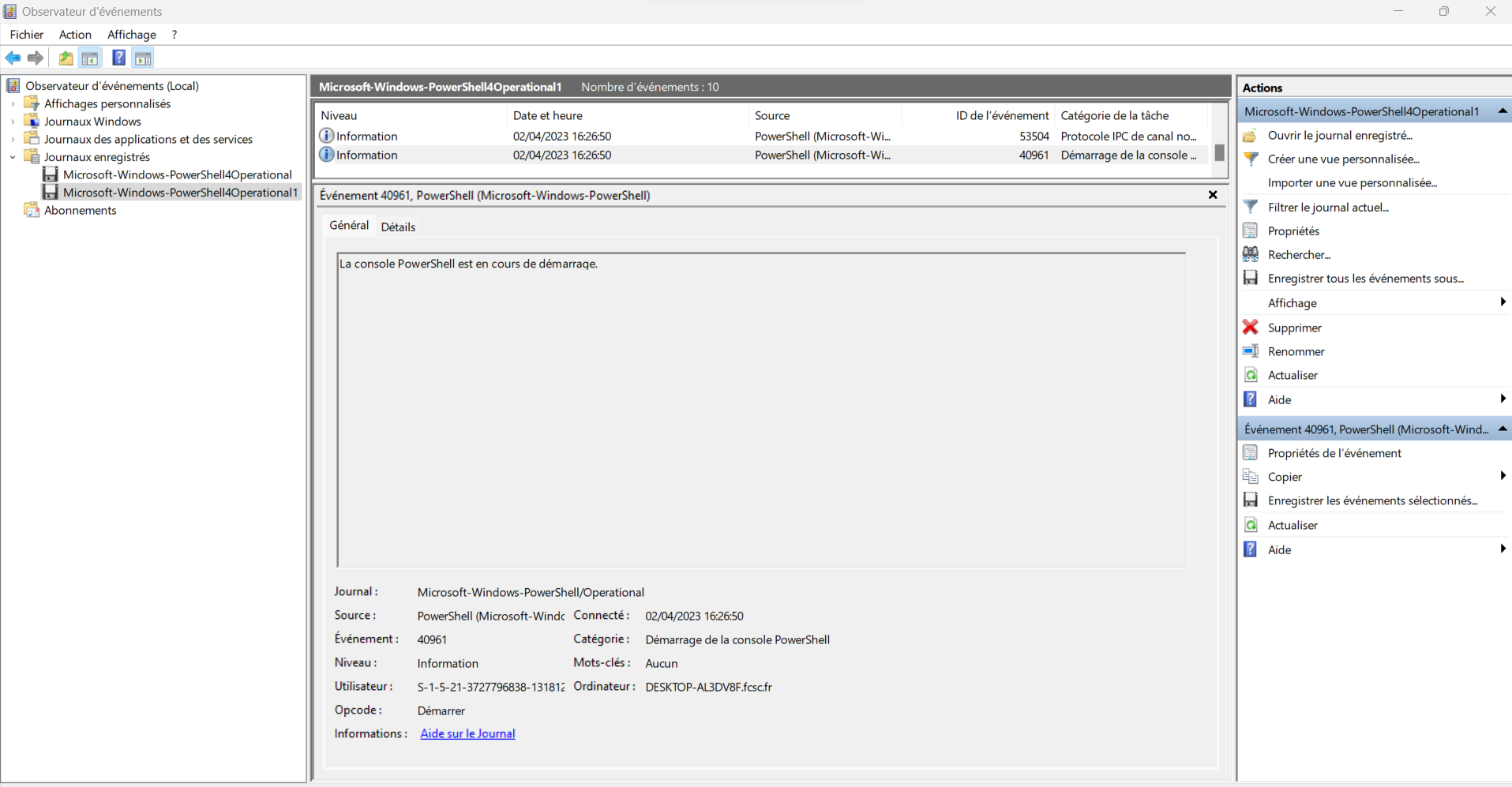
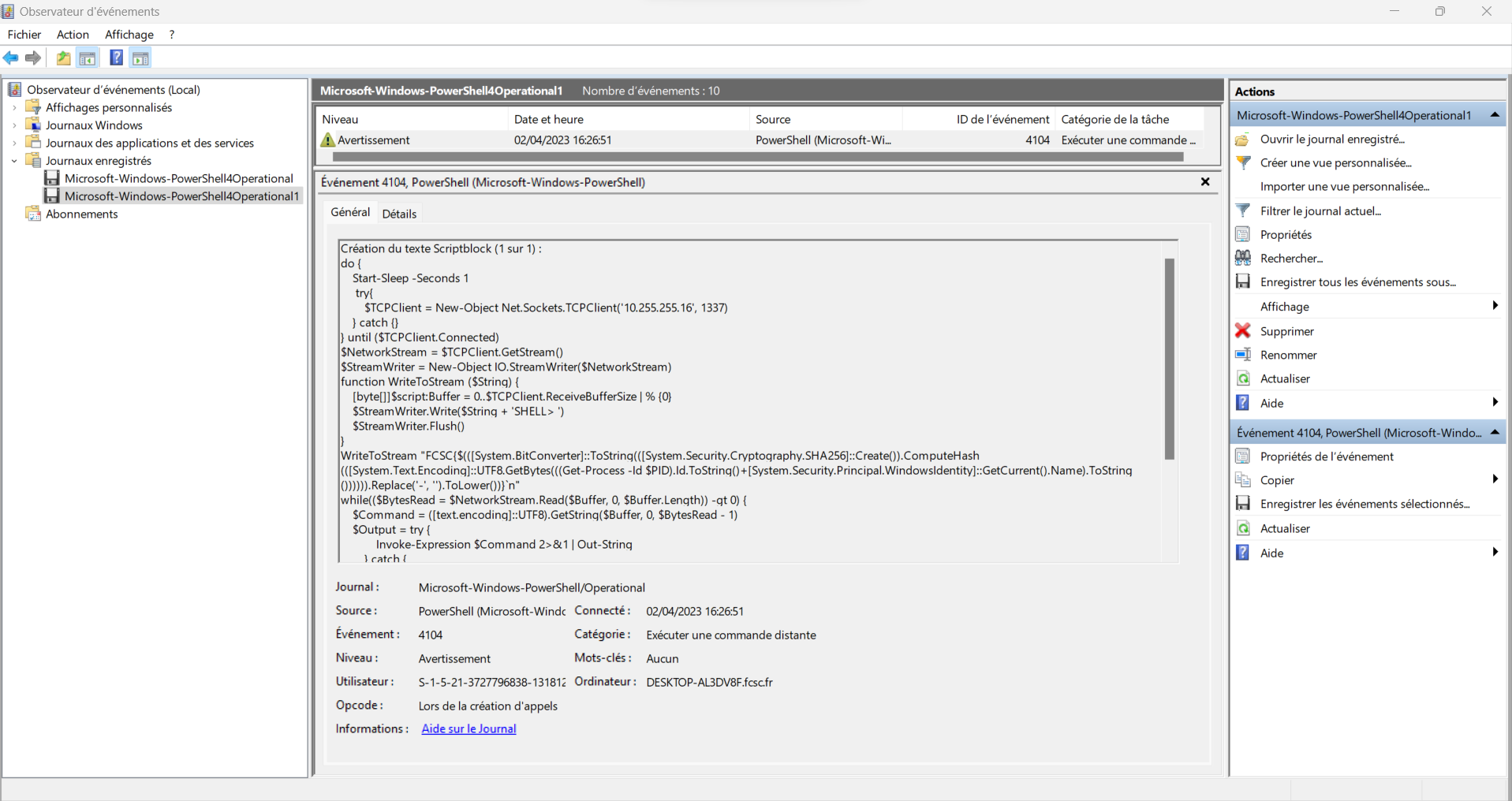


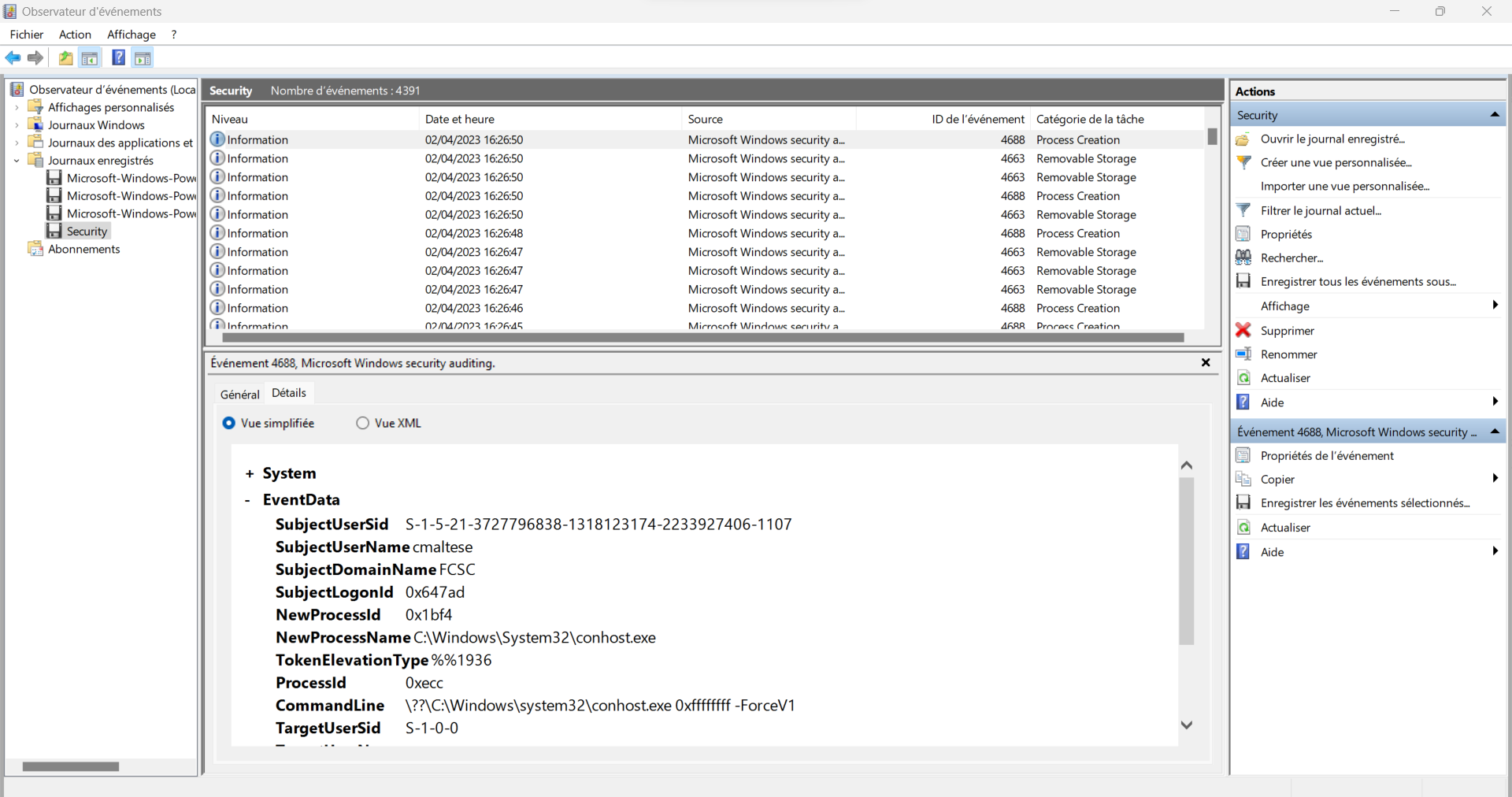




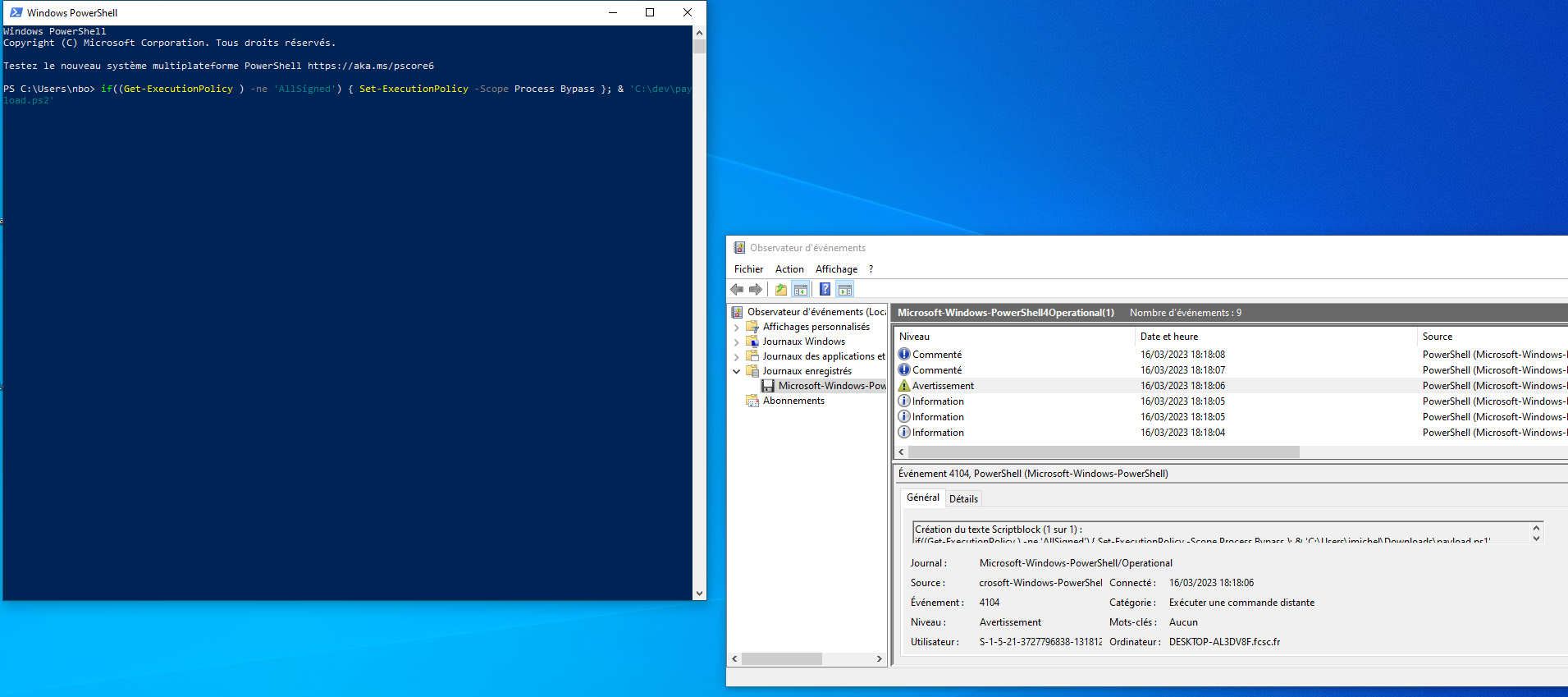
Lançons (côté client): le processus Microsoft-Windows-PowerShell4Operational1 et Security

* 
* 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.
* 

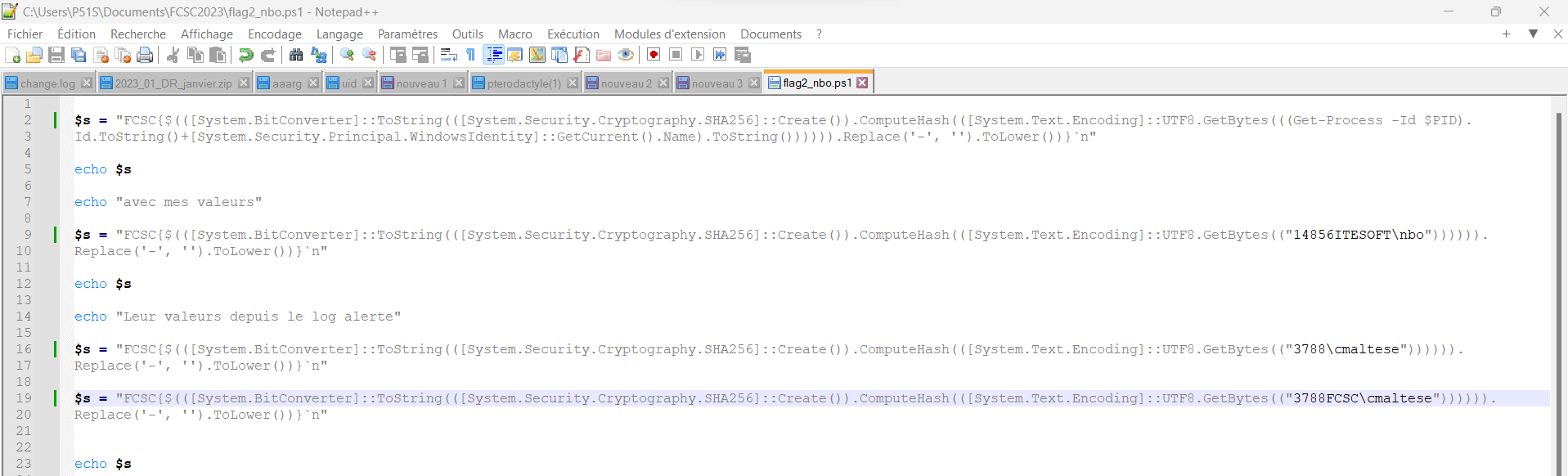




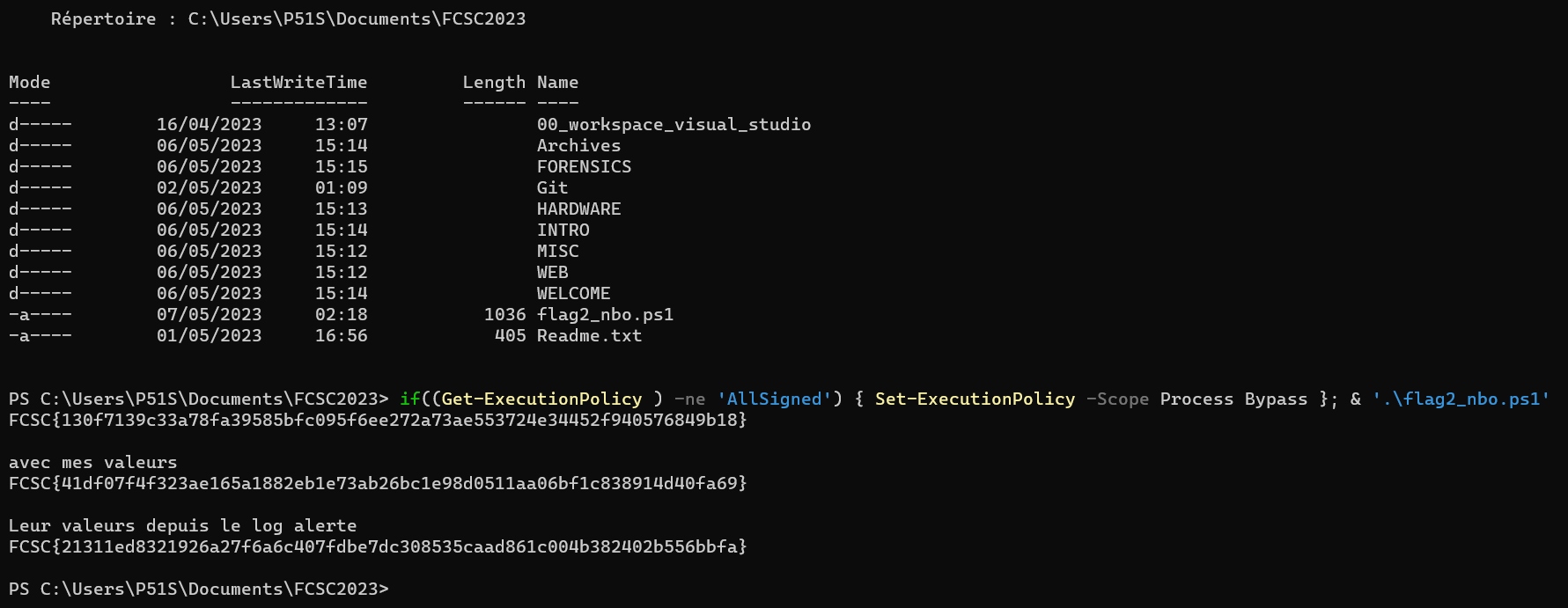
Un essai d’envoi et réception de flag FCSC{…} s’obtient à substituer les champs par des valeurs locales.



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.

