

### ⌚ Objectifs du TP

- Accéder au journal Sécurité d'un contrôleur de domaine
- Filtrer les évènements par ID
- Comprendre les évènements 4624 / 4625 / 4723 / 4724
- Différencier une connexion réussie / échouée
- Identifier le type de connexion (Console, Réseau, RDP)
- Trouver l'adresse IP d'origine d'une connexion
- Analyser les raisons d'un échec
- Utiliser PowerShell pour automatiser l'analyse
- Surveiller les connexions RDP (LogonType = 10)

### 💡 PRÉREQUIS

- 1 serveur Windows Server 2025 Core (SRV)
- Domaine : **sisr.local**
- 1 poste client Windows 10/11 joint au domaine
- Les utilisateurs du fichier CSV déjà importés
- Audit activé (via auditpol)
- RDP et SSH activés pour pouvoir tester les connexions

### ⌚ PARTIE 1 – Découverte des logs avec la console Event Viewer

Même si ton serveur est en mode Core, le **client Windows 10/11** peut ouvrir l'Observateur d'évènements du serveur AD.

#### ✓ Étape 1 – Ouvrir l'Observateur d'évènements

Sur ton poste client :

1. Ouvre **eventvwr.msc**
2. Menu → **Action**  
→ **Se connecter à un autre ordinateur...**
3. Renseigner :  
**srv.sisr.local**

#### ✓ Étape 2 – Localiser le journal Sécurité

Chemin :

Journaux Windows → Sécurité

#### ✓ Étape 3 – Filtrer les évènements

1. Clic droit → **Filtrer le journal...**
2. Dans **ID d'évènement**, entrer :  
**4624,4625,4723,4724**
3. Cliquer **OK**

#### ✓ Étape 4 – Ouvrir un évènement 4624 (connexion réussie)

Dans la partie basse :

- lire **TargetUserName**
- lire **IpAddress**
- lire **LogonType**

#### ✓ Étape 5 – Ouvrir un évènement 4625 (connexion échouée)

- Trouver **Status / SubStatus**
- Noter la raison de l'échec (étape expliquée plus bas avec PowerShell)

## PARTIE 2 – Réaliser des tests de connexion

Pour générer **de vrais évènements**, effectue les actions suivantes depuis le poste client :

### ✓ 1. Connexion réussie

Se connecter au domaine avec un utilisateur du CSV :

SISR\jdupont

Mot de passe correct

### ✓ 2. Connexion échouée

Refaire un essai avec un mauvais mot de passe :

SISR\jdupont

Mot de passe erroné

### ✓ 3. Connexion RDP

Ajouter l'utilisateur plemaire dans le groupe « Admins du domaine »

*Add-ADGroupMember -Identity "Admins du domaine" -Members "plemaire"*

Depuis ptech :

Connexion Bureau à Distance → SRV

Indique : SISR\plemaire

(mot de passe correct puis incorrect)

### ✓ 4. Tentative de changement de mot de passe (4723)

Sur PC client :

Ctrl + Alt + Suppr → Modifier le mot de passe

### ✓ 5. Tentative de réinitialisation de mot de passe (4724)

Sur SRV:

`Set-ADAccountPassword jdupont -Reset -NewPassword (ConvertTo-SecureString "Test1234!" -AsPlainText -Force)`

Cela génère un **4724**.

## PARTIE 3 – Analyse avec PowerShell

Toutes les commandes se font sur :

➔ le serveur **SRV**, en mode Core

OU

➔ le poste client en PowerShell avec accès distant

### ✓ Étape 1 – Lister les 20 derniers évènements du journal Sécurité

`Get-WinEvent -LogName Security -MaxEvents 20 |`

`Select-Object TimeCreated, Id, Message |`

`Format-Table -Wrap`

→ Vérifie que tu vois bien des **4624 / 4625 / 4723 / 4724**.

### ✓ Étape 2 – Filtrer les évènements du domaine SISR (méthode simple)

`Get-WinEvent -LogName Security |`

`Where-Object { $_.Id -in 4624,4625,4723,4724 } |`

`Select-Object TimeCreated, Id, Message |`

`Format-Table -Wrap`

## ⌚ PARTIE 4 – Exécution du Script d’Audit

Voici la version sans commentaires internes.

### ► Script : Analyse des évènements AD sur 2 mois

```
$Depuis = (Get-Date).AddMonths(-2)
```

```
$DomainNetbios = "SISR"
```

```
function Get-EventField {
    param([string]$Name, $Data)
    ($Data | Where-Object { $_.Name -eq $Name } | Select-Object -First 1).'#text'
}

function Get-ReasonFromStatus {
    param([string]$Status, [string]$SubStatus)
    switch ($SubStatus) {
        '0xC000006A' { "Mot de passe incorrect" }
        '0xC0000064' { "Utilisateur inexistant" }
        '0xC0000234' { "Compte verrouillé" }
        '0xC0000072' { "Compte désactivé" }
        default {
            if ($Status -or $SubStatus) {
                "Status=$Status / SubStatus=$SubStatus"
            }
        }
    }
}

function Get-LogonTypeDetail {
    param([string]$LogonType)
    switch ($LogonType) {
        '2' { "Interactive (console)" }
        '3' { "Network (SMB)" }
        '10' { "RemoteInteractive (RDP)" }
        default { "Type inconnu ($LogonType)" }
    }
}

$filtre = @{
    LogName  = 'Security'
    Id       = 4624,4625,4723,4724
    StartTime = $Depuis
}

Get-WinEvent -FilterHashtable $filtre |
Sort-Object TimeCreated |
ForEach-Object {

    $xml = [xml]$_.ToXml()
    $data = $xml.Event.EventData.Data
```

```

$eventId = $_.Id
$time    = $_.TimeCreated
$targetUser = Get-EventField 'TargetUserName' $data
$targetDom = Get-EventField 'TargetDomainName' $data
$ip      = Get-EventField 'IpAddress'     $data
$machine = Get-EventField 'WorkstationName' $data
$logonType = Get-EventField 'LogonType'     $data

if ($targetUser -match '\$\$') { return }
if ($targetDom -and $targetDom -ne $DomainNetbios) { return }

$ipv4 = if ($ip -match '^\\d{1,3}(\\.\\d{1,3}){3}\\$') { $ip } else { $null }
$status = Get-EventField 'Status' $data
$subStatus = Get-EventField 'SubStatus' $data
$raison = $null
$action = $null

switch ($eventId) {
    4624 { $action = "Connexion réussie" }
    4625 {
        $action = "Connexion échouée"
        $raison = Get-ReasonFromStatus $status $subStatus
    }
    4723 { $action = "Changement de mot de passe" }
    4724 { $action = "Réinitialisation de mot de passe" }
}

[PSCustomObject]@{
    DateHeure   = $time
    EventID     = $eventId
    Utilisateur = $targetUser
    Machine     = $machine
    IPv4        = $ipv4
    TypeLogon   = $logonType
    TypeLogonDetail= Get-LogonTypeDetail $logonType
    Action       = $action
    Raison      = $raison
}

} | Format-Table -AutoSize
A enregistrer sous : Audit-Connexions.ps1

```

## PARTIE 5 – Interprétation et questions guidées

### **1 Trouver toutes les connexions RDP**

👉 Indice : LogonType = 10

**Question :**

Quel utilisateur s'est connecté en RDP ?

Depuis quelle machine ?

À quelle heure ?

### **2 Trouver les connexions échouées (4625)**

**Question :**

Pour l'utilisateur *jdupont*, quelle est la raison de l'échec ?

(voir colonne **Raison**)

### **3 Trouver les tentatives de changement de mot de passe (4723)**

**Question :**

Quel utilisateur a tenté de changer son mot de passe ?

Depuis quel poste ?

### **4 Trouver les réinitialisations (4724)**

**Question :**

Quel compte a été réinitialisé ?

Par qui ?

### **5 Trouver toutes les IP ayant tenté une connexion**

**Question :**

Quelles adresses IP apparaissent dans les logs ?

Y a-t-il des IP suspectes ?

## PARTIE 6 – Synthèse à rendre

Rédiger un rapport contenant :

- les événements détectés
- les explications (succès / échec / RDP / changement / reset)
- les IP sources
- les conclusions
- un schéma simple du cycle :  
Tentative → Analyse → Diagnostic → Remédiation