# Résolution de l’Analyse Forensique : Forensic et Mat [2/2]

Le journal des événements : CTFCORP_Security.evtx est plus dense que le précédent .

Nous devons retrouver un événement d’une tâche effectuant une tentative d’effacement.

Le format du flag est ceci : 404CTF{IP-PORT-USER-TASKNAME-TIMESTAMP-GROUP}

Il y a des tas d’IP et de login d'escalade mais si on parle de tâche et de persistant, il n'y a que celle figurant ci-dessous ou avec une IP locale ; mais pas très cohérente « a priori ».

Or, l’utilisateur=svc-x persistant depuis IP=10.66.77.88:4444 [Type: 3] Administrateurs

404CTF{10.66.77.88-4444-svc-x-WinUpdate_Check_75312-1747245631-Administrateurs},

404CTF{10.66.77.88-4444-svc-x-WinUpdate_Check_75312-1747255228-Administrateurs},

404CTF{10.66.77.88-4444-svc-x-WinUpdate_Check-1747245631-Administrateurs}

404CTF{10.66.77.88-4444-svc-x-WinUpdate_Check-1747255228-Administrateurs}

**Ce que prouvent les logs CTFCORP_Security.evtx**

1. **Tentative d’effacement des journaux (échouée)**

- Processus observé : C:\Windows\System32\wevtutil.exe avec **Status = 0xC0000022** (Access Denied).
- Interprétation : wevtutil cl <LogName> sert à **vider un journal d’événements** ; l’opération **exige des droits** (Clear permission / admin). Ici, l’essai a échoué (0xC0000022 = STATUS_ACCESS_DENIED). https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/wevtutil

2. **Connexion réseau de svc-x depuis une machine cliente**

- Événement **4624** (*successful logon*) avec **LogonType = 3**, **AuthenticationPackage = NTLM**, **WorkstationName = WORKSTATION-596**, **IpAddress = 10.66.77.88**, **IpPort = 4444**.
- Interprétation : 4624 atteste d’une **ouverture de session réussie** ; le **LogonType 3** correspond à une **connexion réseau** (ex. accès à distance/partage), et les champs IP/Port/Workstation identifient la source. https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4624

3. **Création d’une tâche planifiée malveillante**

- Événement **4698** (*A scheduled task was created*) pour \WinUpdate_Check_75312, avec un **TaskContent** qui lance powershell.exe et **Arguments** pointant vers C:\Users\svc-x\AppData\Local\Temp\payload.ps1 (déclenchée au **Boot**).
- Interprétation : l’ID 4698 se déclenche **à chaque création** de tâche planifiée ; ici elle persiste au redémarrage et **exécute un script PowerShell**. https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4698

4. **Exécution de PowerShell par le moteur des tâches**

- Événement **4688** (*A new process has been created*) :
    - ParentProcessName = C:\Windows\System32\taskeng.exe
    - NewProcessName = ...\powershell.exe
    - CommandLine = -WindowStyle Hidden -ExecutionPolicy Bypass -File ...\payload.ps1
- Interprétation : 4688 **journalise chaque programme lancé** et permet la **corrélation par PID** (utile pour relier ce lancement aux autres actions du même processus). https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4688

5. **Élévation de privilèges locale**

- Événement **4732** (*A member was added to a security-enabled local group*) : l'utilisateur **svc-x** est ajouté au **groupe local Administrateurs** (SID **S-1-5-32-544**).
- Interprétation : 4732 s'émet **lorsqu'un membre est ajouté** à un groupe local de sécurité ; ici, l'ajout à *Administrateurs* donne des **privilèges étendus** sur l'hôte. https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4732

**Chronologie extraite des horodatages (UTC)**

- 18:00:24 — **4732** : svc-x ajouté aux **Administrateurs**.
- 18:00:28 — **4698** : création de la tâche \WinUpdate_Check_75312 (**payload.ps1** au démarrage).
- 18:00:31 — **4688** : **taskeng.exe** lance **powershell.exe** avec **payload.ps1** (bypass + caché).
- 18:00:33 — **wevtutil.exe** tente de **purger les journaux** ⇒ **refusé (0xC0000022)**.

L'ensemble montre clairement : **compromission du compte svc-x**, création d'une **tâche persistante** exécutant un **payload PowerShell**, **élévation de privilèges** locale, **activité réseau** (LogonType 3, **10.66.77.88:4444**), puis **tentative d'effacement de traces** avortée.

**Conversion d'horodatage → epoch (pour le flag)**

Tu as retenu l'horodatage de création de la tâche :
**2025-05-14T18:00:28.1141208Z → 1747245628** (arrondi/seconde).
(Ex. sous Linux : date -d '2025-05-14 18:00:28Z' +%s.)

**Pas à pas — ce que fait le script pour la conversion**

1. **Extrait** l'attribut SystemTime dans l'XML d'un événement (System/TimeCreated). (Dans l'Observateur d'événements en mode XML, tu vois bien l'Z = UTC.) https://learn.microsoft.com/en-us/answers/questions/2705675/system-time-in-event-viewer

2. **Parse** la chaîne ISO 8601 :
    - en **3.11+**, fromisoformat() comprend Z ;
    - sinon, **remplace Z par +00:00** pour obtenir un datetime « aware » UTC. https://stackoverflow.com/questions/75867446/documentation-example-for-datetime-fromisoformat-raises-invalid-isoformat-string
3. **Convertit** en **epoch** avec : .timestamp() et **prend l'entier** attendu dans ton CTF. L'epoch côté Python et POSIX est bien **UTC** sans secondes intercalaires.

    Il suffit d'une routine de script en python pour décoder le champ EventTimestamp.

Combiner ensuite les données rassemblées pour en obtenir le résultat (drapeau ou flag).

**Le Flag (éléments concaténés dans l'ordre demandé)**

404CTF{10.66.77.88-4444-svc-x-WinUpdate_Check_75312-1747245628-Administrateurs}