PROJET : RÉALISATION ET DÉTECTION D'UNE ATTAQUE AVEC MITRE ATT&CK ET WAZUH EDR

MITRE ATT&CK® est une base de connaissances mondialement accessible sur les tactiques et les techniques des adversaires, basée sur des observations du monde réel. La base de connaissances ATT&CK est utilisée comme fondement pour le développement de modèles et de méthodologies de menaces spécifiques dans le secteur privé, les gouvernements et dans la communauté des produits et services de cybersécurité.

CONTEXTE

Dans ce projet nous allons réaliser une attaque qui va exécuter par procuration un code malveillant sur une machine cible avec l'exécutable **Regsvr32.exe**

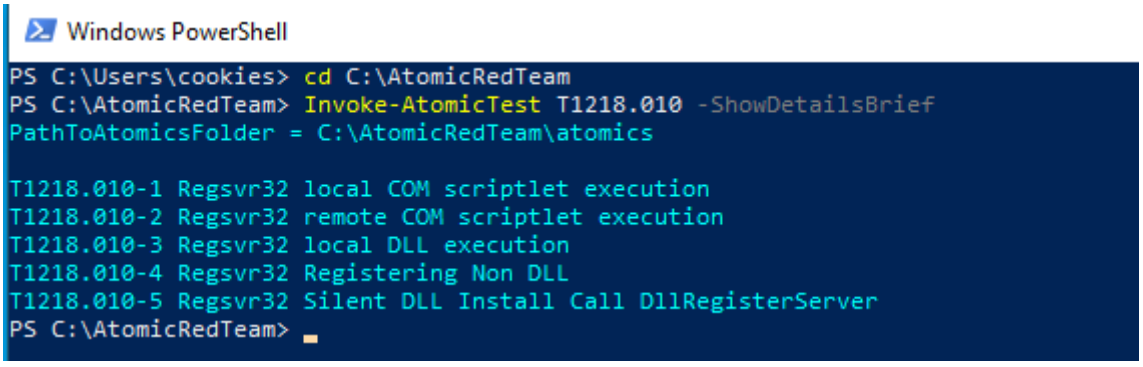
Regsvr32.exe est un programme de ligne de commande utilisé pour enregistrer et désenregistrer les contrôles de liaison et d'intégration d'objets, y compris les bibliothèques de liens dynamiques (DLL), sur les systèmes Windows.

Après l'exécution de ce programme, **calc.exe** (l'application calculatrice) sera lancée automatiquement dans la machine cible.

Notre objectif dans ce projet sera la détection de cette attaque par notre EDR (Endpoint Detection and Response) WAZUH.

PARTIE 1 : PRÉPARATION DE L'ATTAQUE AVEC ATOMIC RED TEAM

L'attaque est enregistrée sur MITRE ATT&CK avec la référence **T1218.010-3 (Regsvr32 local DLL execution).**



```
PS C:\AtomicRedTeam> Invoke-AtomicTest T1218.010 -TestNumbers 3 -ShowDetails
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

[********BEGIN TEST*******]
Technique: Signed Binary Proxy Execution: Regsvr32 T1218.010
Atomic Test Name: Regsvr32 local DLL execution
Atomic Test Number: 3
Atomic Test GUID: 08ffca73-9a3d-471a-aeb0-68b4aa3ab37b
Description: Regsvr32.exe is a command-line program used to register and unregister OLE controls. Upon execution, calc.exe will be launched.
```

Maintenant nous allons vérifier si nous disposons des prérequis nécessaires pour lancer l'attaque.

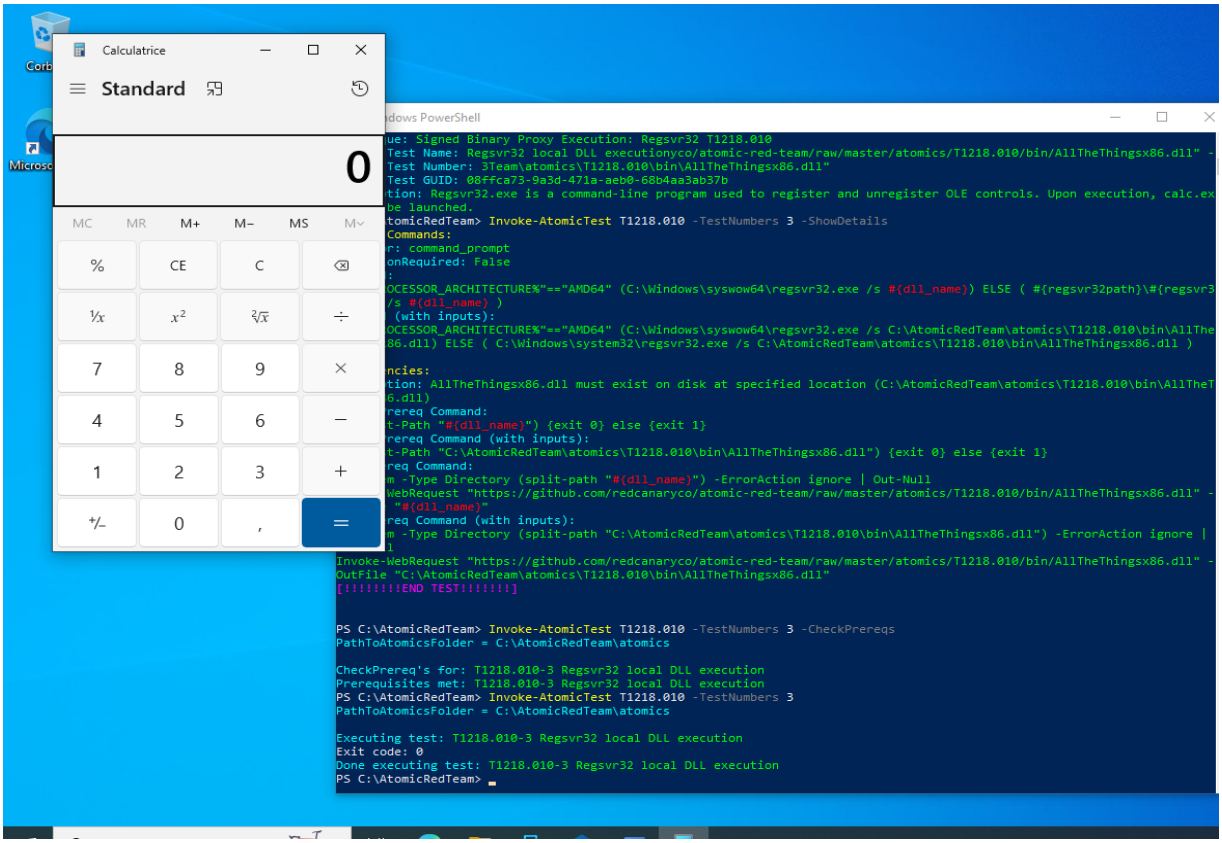
Les prérequis sont satisfaits cela ne nécessite pas de prérequis.

```
PS C:\AtomicRedTeam> Invoke-AtomicTest T1218.010 -TestNumbers 3 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1218.010-3 Regsvr32 local DLL execution
Prerequisites met: T1218.010-3 Regsvr32 local DLL execution
```

PARTIE 2 : LANCEMENT DE L'ATTAQUE

Après vérifications des prérequis, l'attaque a pu être lancé avec succès grâce à ATOMIC RED TEAM. Nous pouvons constater qu'après l'exécution de l'attaque l'application calculatrice a été automatiquement lancée dans la machine cible.



<u>PARTIE 3</u> : Détection de l'attaque par WAZUH

Après lancement de l'attaque **T1218.010-3 via** Atomic Red Team, nous constatons que Wazuh n'a rencontré aucune difficulté à la détecter. La capture ci-dessous montre le chemin d'accès du **services.exe**.

t	_index	wazuh-alerts-4.x-2024.08.12
t	agent.id	002
t	agent.ip	192.168.111.133
t	agent.name	mdiaw_windows
t	data.win.eventdata.authenticationPackageName	Negotiate
t	data.win.eventdata.elevatedToken	%%1842
t	data.win.eventdata.impersonationLevel	%%1833
t	data.win.eventdata.keyLength	0
t	data.win.eventdata.logonGuid	{00000000-0000-0000-0000-000000000000}
t	data.win.eventdata.logonProcessName	Advapi
t	data.win.eventdata.logonType	5
t	data.win.eventdata.processId	0x2cc
t	data.win.eventdata.processName	C:\\Windows\\System32\\services.exe
t	data.win.eventdata.subjectDomainName	WORKGROUP
t	data.win.eventdata.subjectLogonId	0x3e7
t	data.win.eventdata.subjectUserName	DESKTOP-6P2QUEG$
t	data.win.eventdata.subjectUserSid	S-1-5-18