**windows persistence**

بسم الله الرحمن الرحيم

**وش يعني persistence**

لما تخترق جهاز و تتحكم فيه اول ما يتسكر الجهاز راح يروح الشل حقك ف لازم نخلي الجهاز اول ما يشتغل يروح و يشغل ال backdoor حقنا

​

**Windows folder**

C:\Users\%USER%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

​

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

اي ملف نحطه في هذا المسار راح يشتغل

Text

Description automatically generated

الحين حطيت calc.exe في المجلد هذا بسكر الجهاز و بشغله اذا اشتغل calc.exe يعني شغلنا صح

Graphical user interface, application

Description automatically generated

اشتغل معنا بشكل طبيعي

**Registry keys**

Computer\HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Computer\HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run

Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\RunOnce

Graphical user interface, text, application, email

Description automatically generated

حطيت calc.exe و بعد اعدت تشغيل الجهاز اشتغل calc.exe و تشتغل بدون اي مشاكل

​

**Scheduled Tasks**

schtasks /create /sc minute /MO 1 /tn "Example\Test" /tr "C:\windows\system32\calc.exe"

A picture containing graphical user interface

Description automatically generated

باستخدام Scheduled Tasks نقدر نخلي calc.exe تشتغل كل دقيقه على سبيل المثال

​

**Services**

Graphical user interface, text, application, email

Description automatically generated

نقدر في windows services اذا صارcrash ل service تشغل برنامج حنا نبيه يعني اذا صار crash ل RDP يشغل shell.exe

​

**DLL hijacking**

كثير من البرامج تكون مصابه ب هذي الثغره و نقدر منها كل ما شغل اليوزر مثلا chrome بشرط انه يكون مصاب يشغل لنا shell.dll

**Shortcut hijacking**

البرامج لما تكون على سطح المكتب تكوت shortcut للمسار الاصلي ف نقدر نتلاعب في shortcut هذا

​

Graphical user interface, text, application, email

Description automatically generated

مثلا عندي chrome.exe راح اتلاعب في shortcut حقه الموجود في سطح المكتب

خليته يشغل ملف powershell و حطيت في ملف powershell

Text

Description automatically generated

و بهذي الطريقه راح يفتح قوقل و يفتح calc.exe انت تقدر تغير و تخليه backdoor حقك حقك

​

**الملخص**

سوينا اكثر من طريقه ل windows persistence هل فيه غيرها؟ فيه كثير غيرها ماشرحت عنها

هل blue team يقدر يكتشفني؟ ايه يقدر و انصحك تجرب برنامج [autoruns](https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns) راح يعطيك كل البرامج اللي صاير لها persistence على جهازك