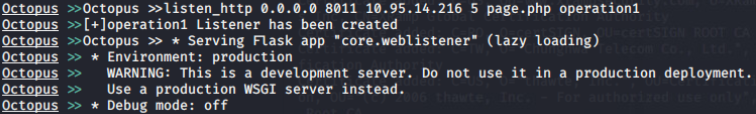
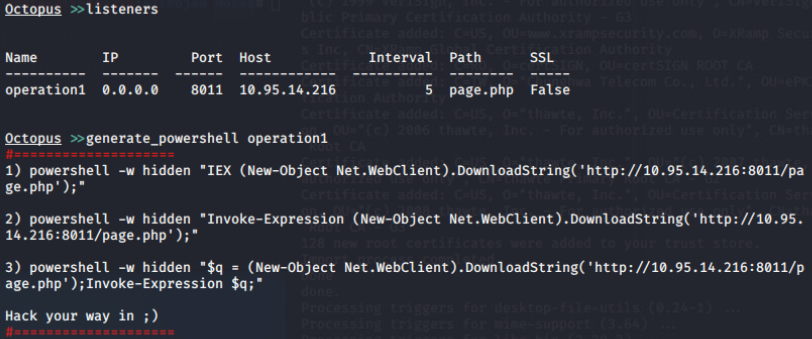
**Octopus:**

Open source pre-operation C2 server based on python and powershell

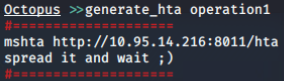
创建监听:



创建agent(powershell):



创建agent(hta):

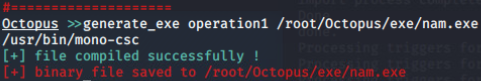


创建agent(exe):

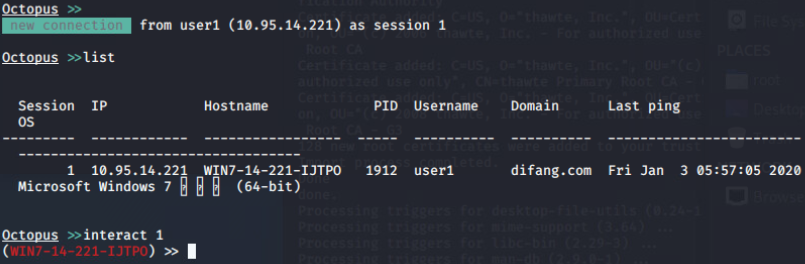
Octopus can build a ready to use windows executable (exe file) for you using mono-project to compile the C# agent to an executable.

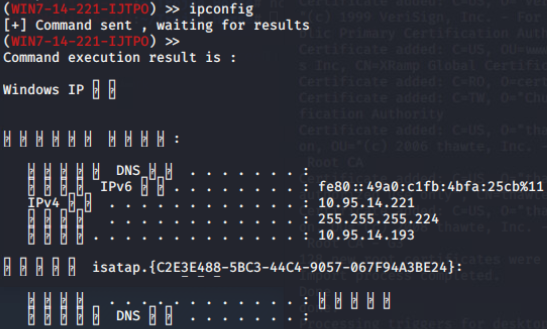
Octopus use a technique called “unmanaged powershell” to execute the powershell script without touching the powershell.exe binary, which can help you to avoid any restrictions on powershell.exe.

Octopus will use “System.Management.Automation.dll” file to compile the C# code and then use the “PowerShell” object to start the powershell code execution.



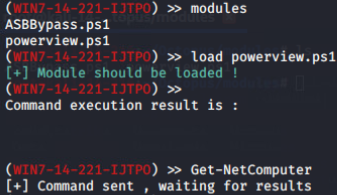
与agent交互:



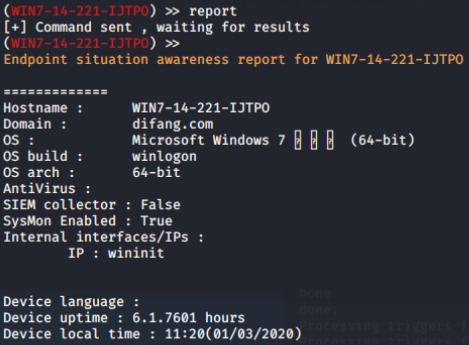


加载外部powershell模块:

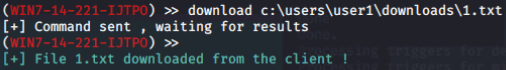




ESA(Endpoint Situational Awareness):



下载文件:



关闭杀软:

