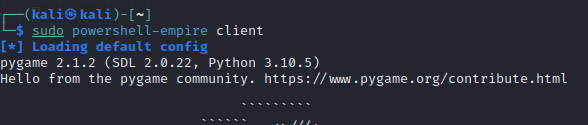
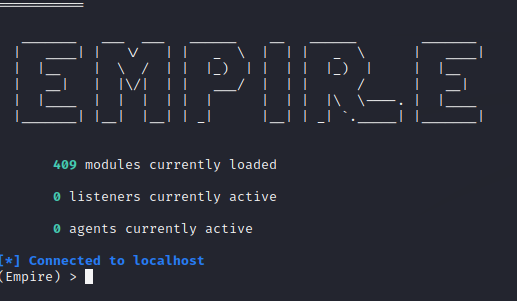
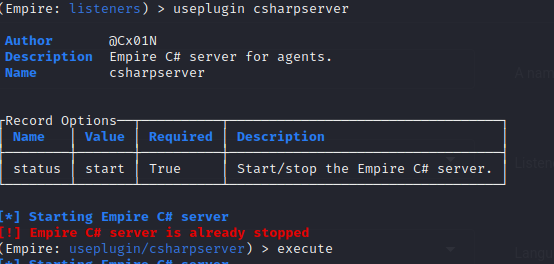
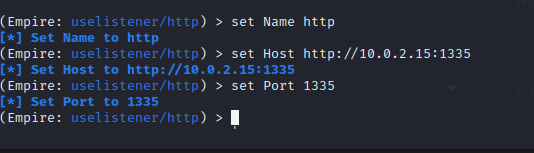


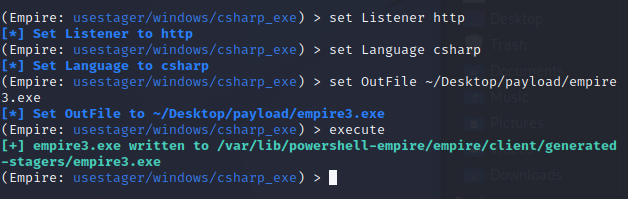
Set up server to be able to connect to the client, to start up the stagers module etc. you can also see the restful api, wheretwo computer systems use to exchange information securely over the internet.



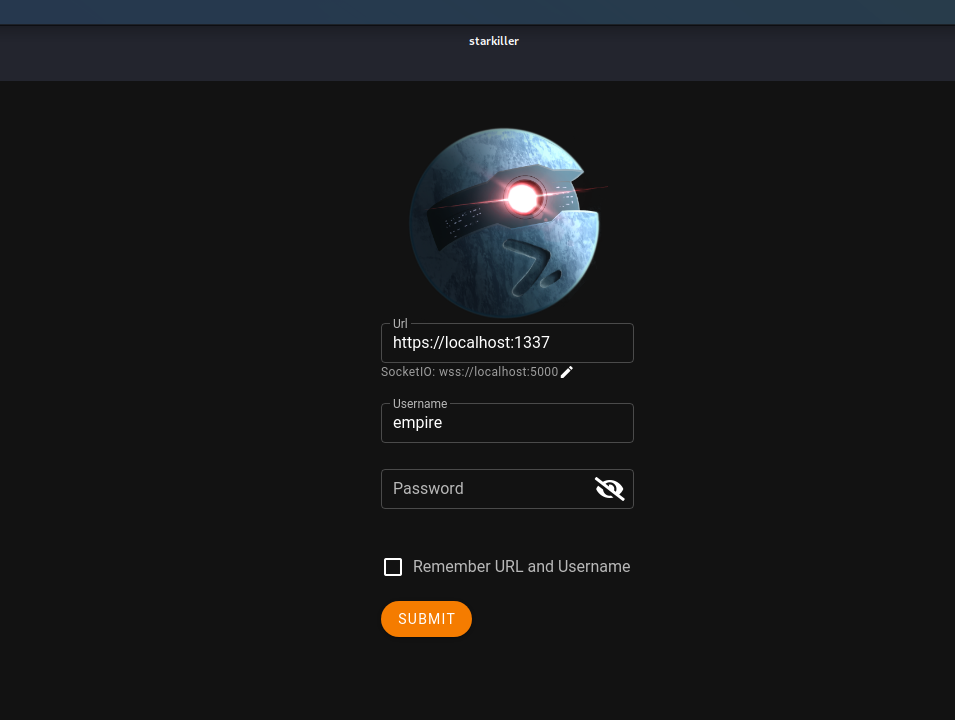




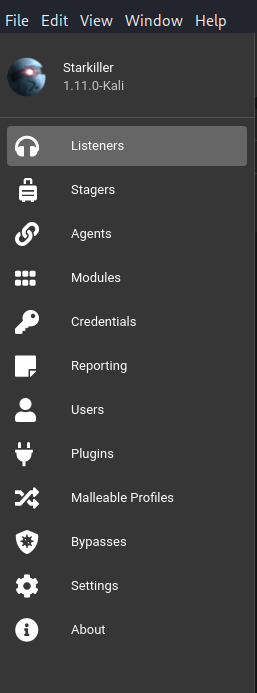


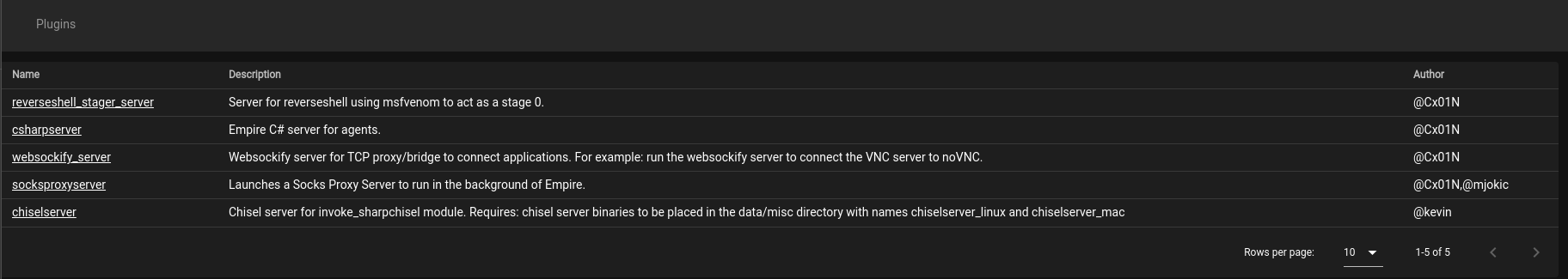


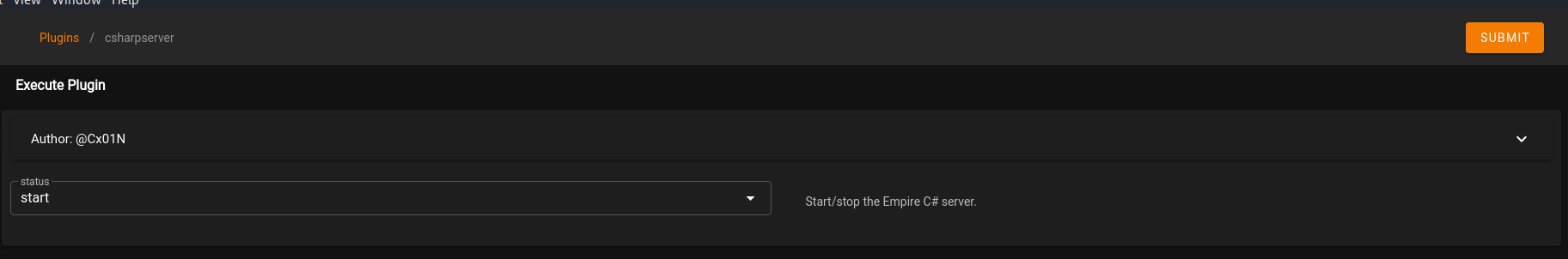
Listener use to listen or watch any connection made to your network.

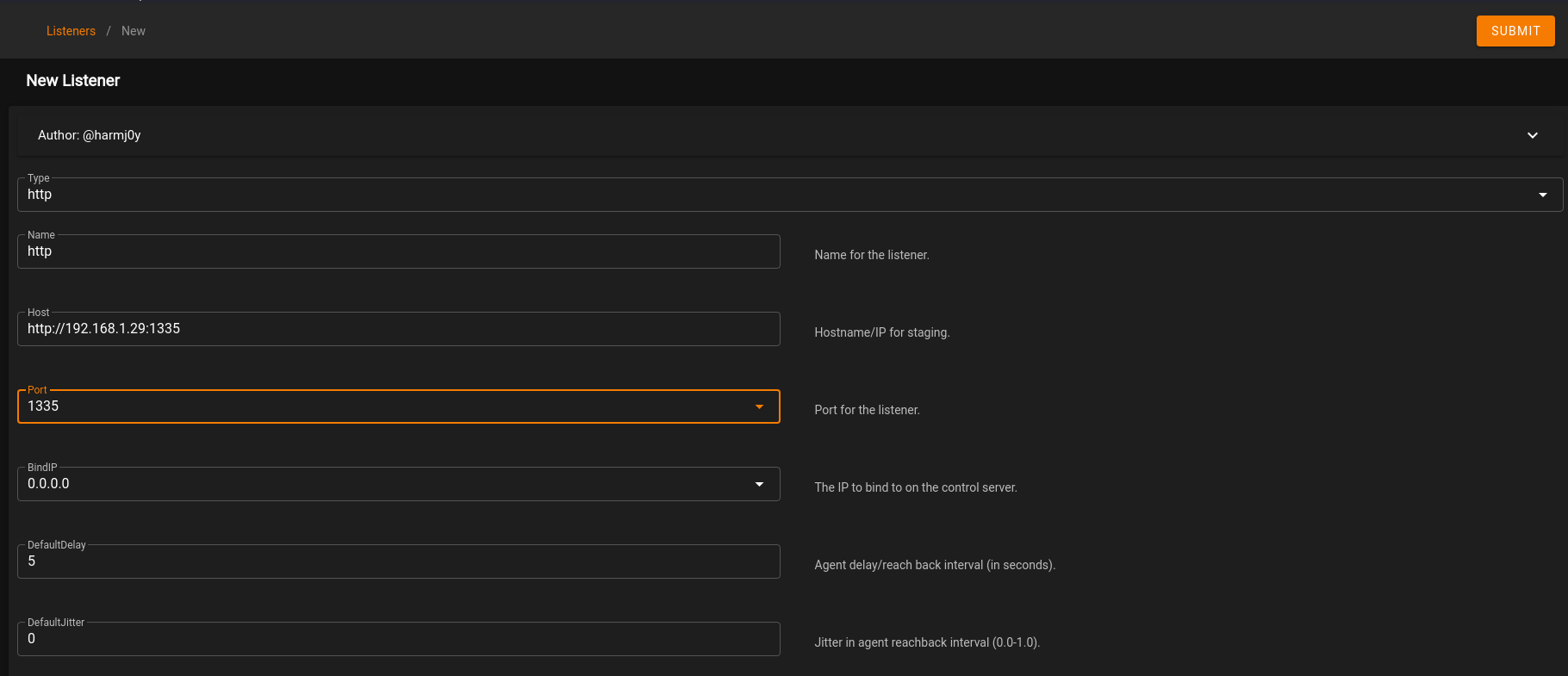
e  
GUI interface for empire.

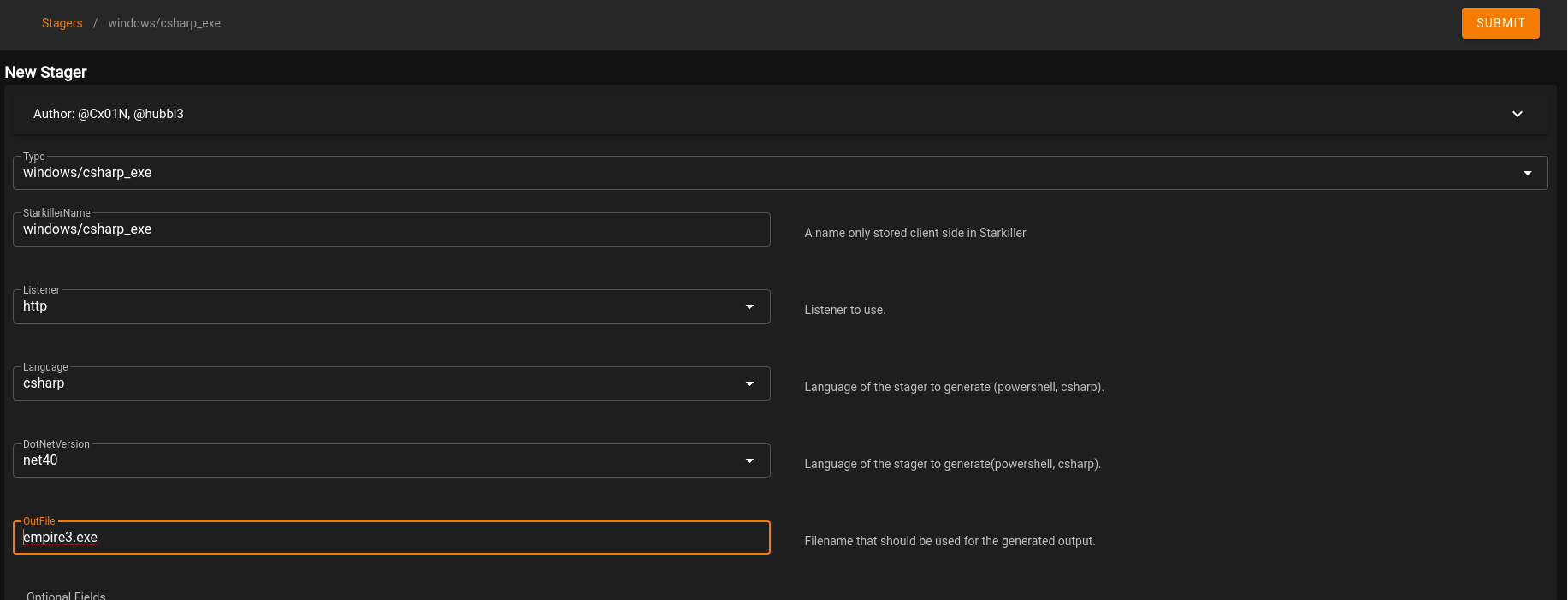
Default user username: empireadmin, password: password123

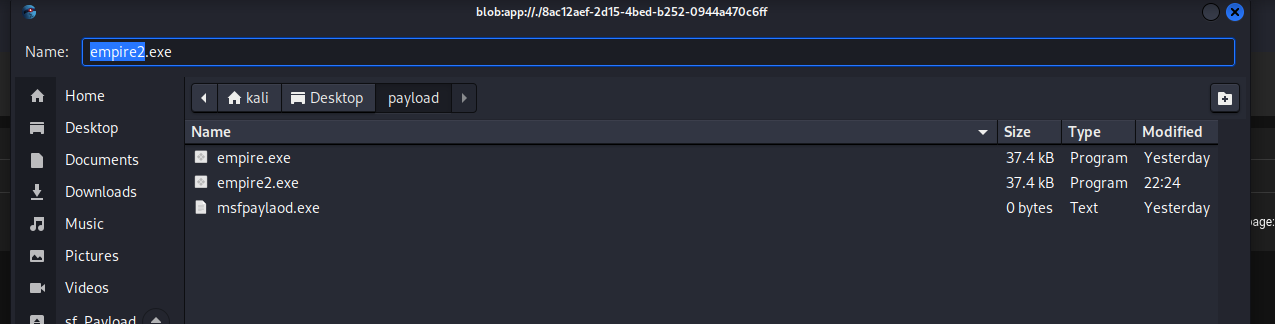
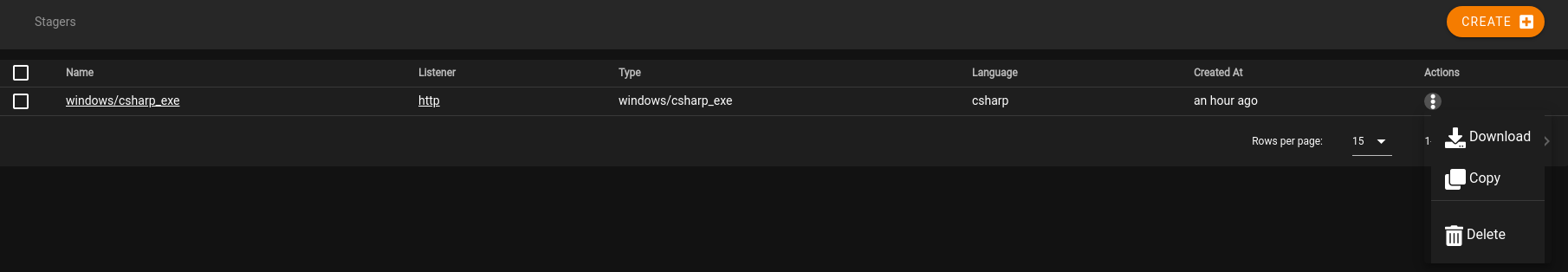


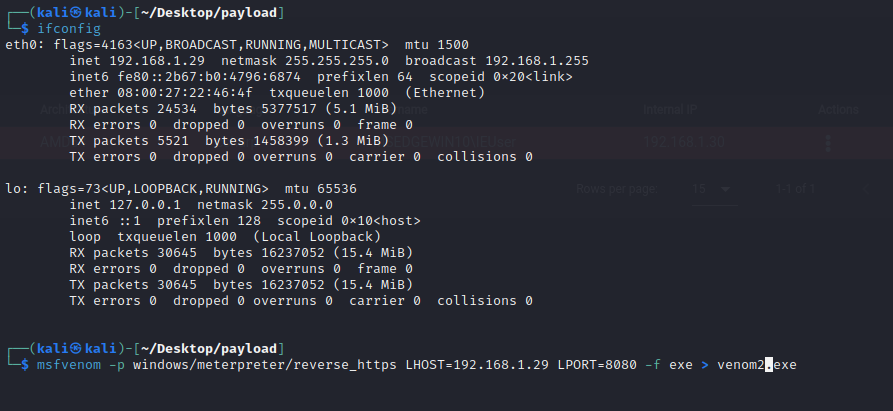


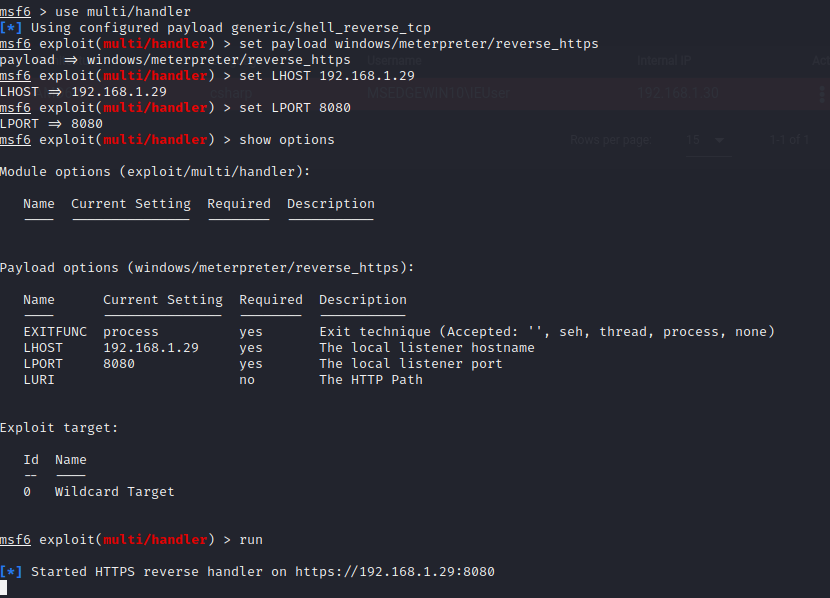






  
  
MSFCONSOLE ~

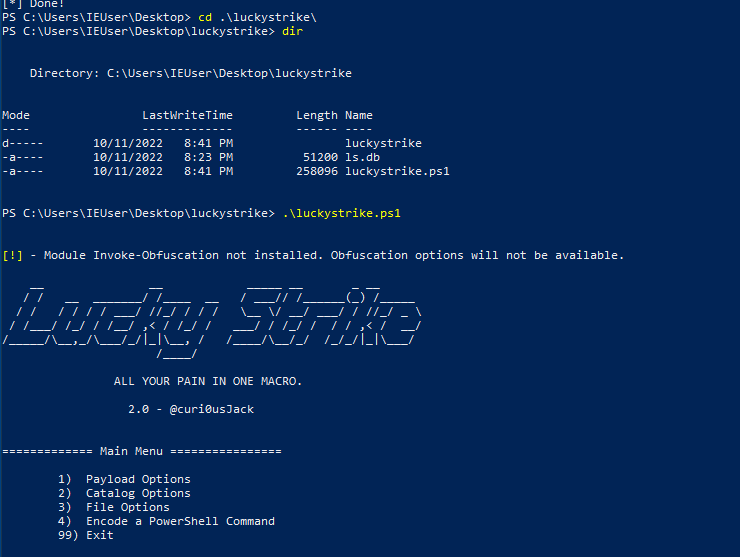
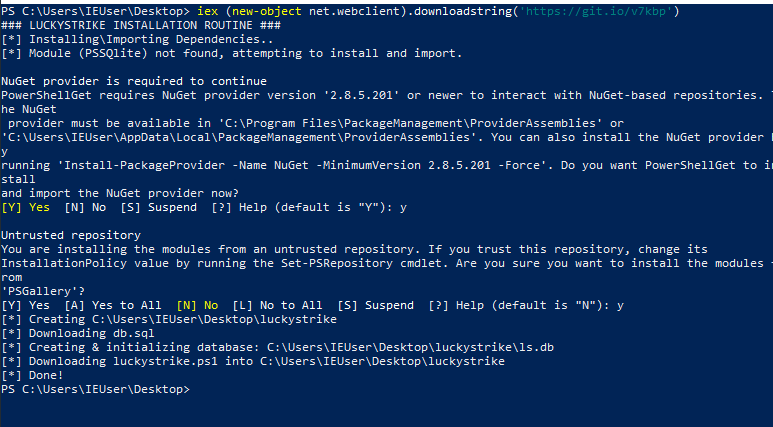
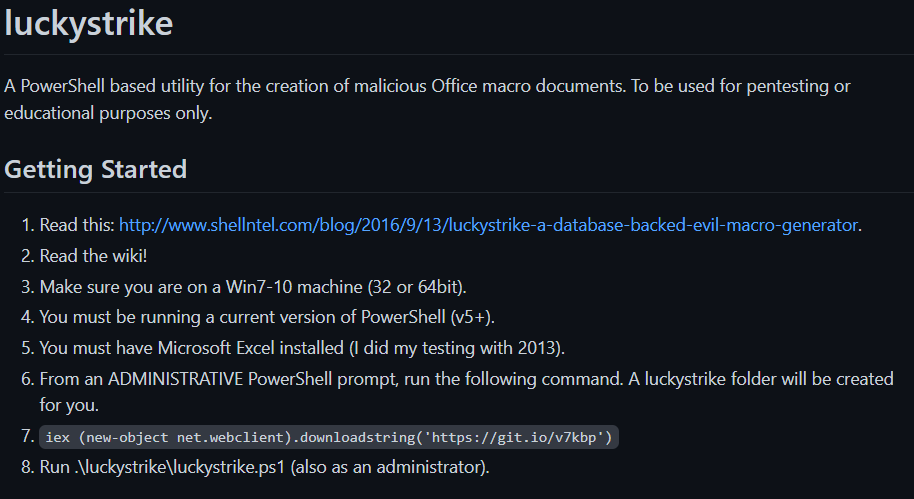


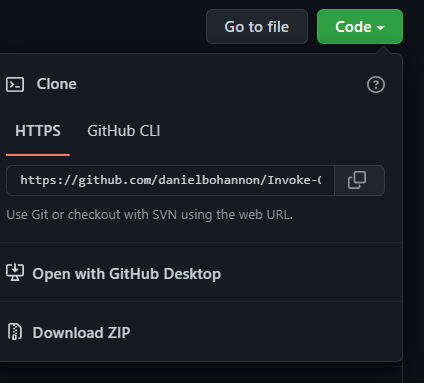


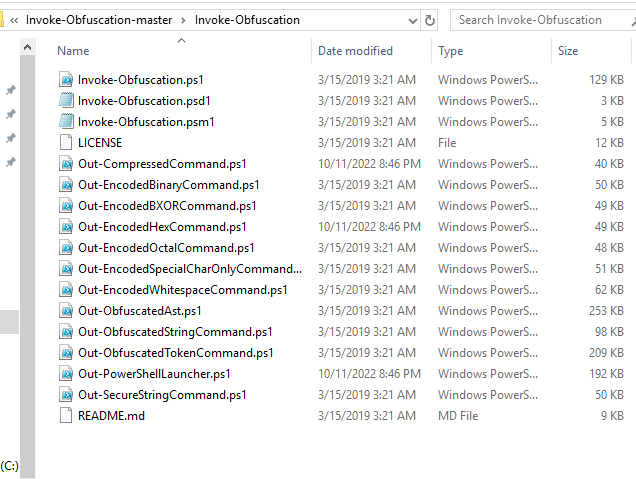
Lucky strike

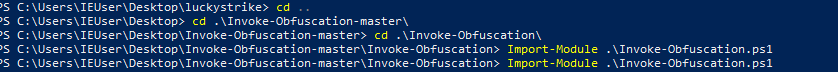
<https://github.com/curi0usJack/luckystrike>

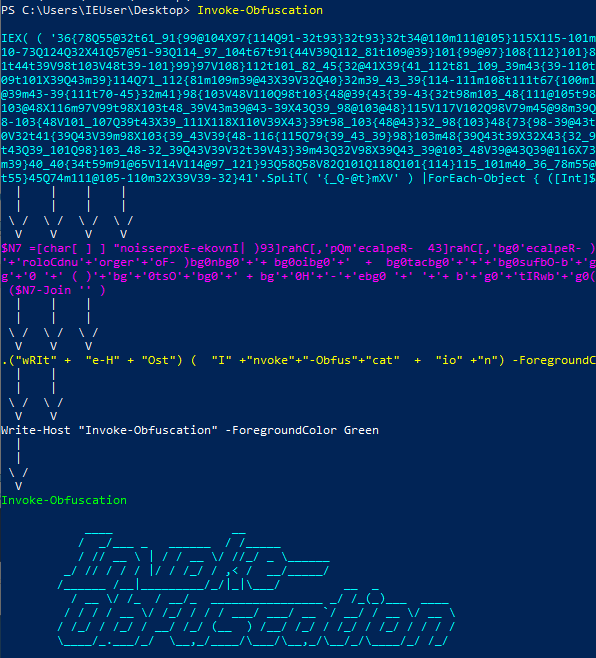
Make sure before you download, you have your windows defender off



You would notice it Invoke-Obfuscation is not installed, you can download it and install to a github repo.  
Invoke-obfuscation module is the one that would hide, encrypt, tokenization, and data masking.



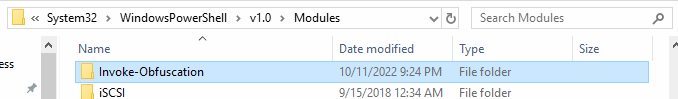
  
For this Invoke-Obfuscation were gonna use the Invoke-Obfuscation.ps1



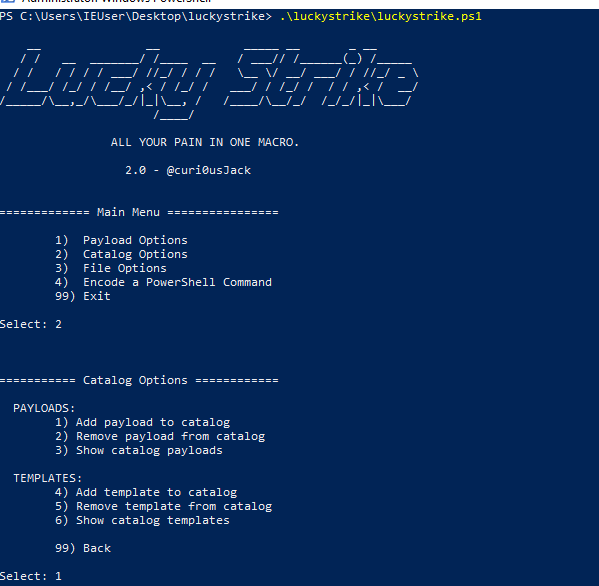
After Confirming that it works. You can now add the module to the powershell modules

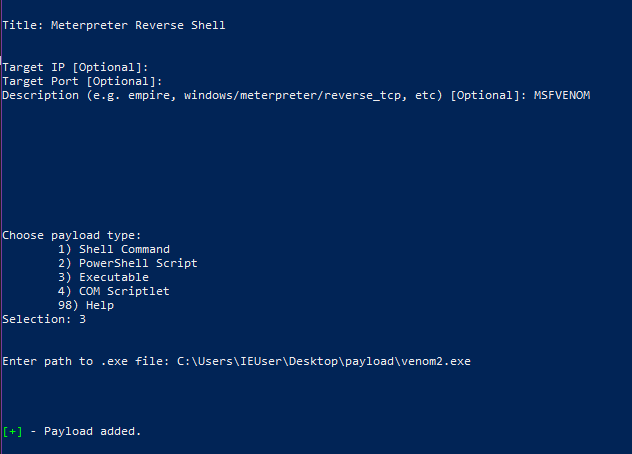
Invoke-Obfuscation

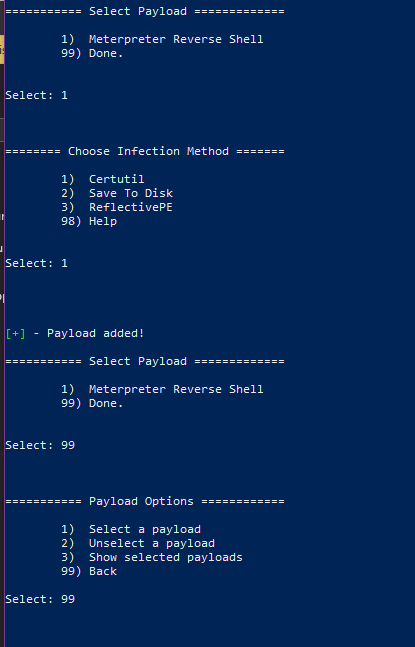
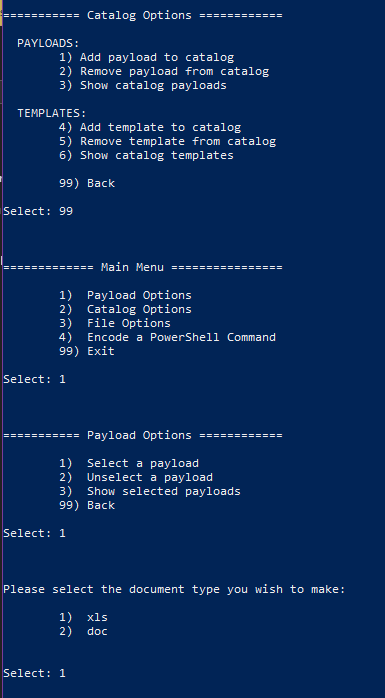
Attackers and commodity malware have started using extremely basic obfuscation techniques to hide the majority of the command from the command line arguments of powershell.exe.

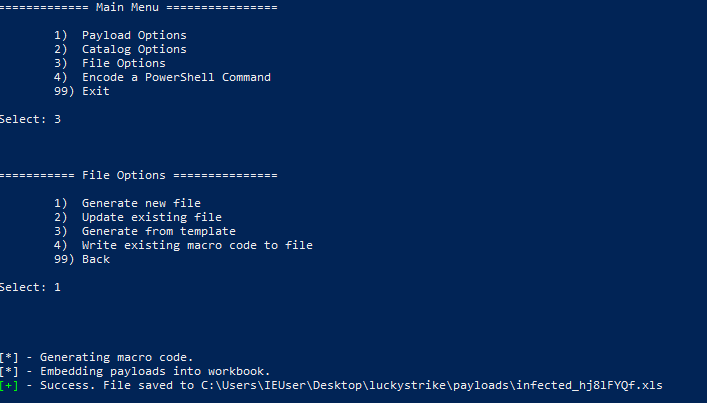


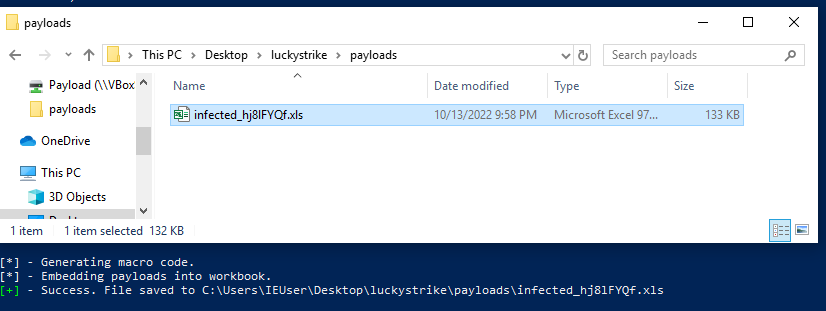
LUCKY STRIKE Metasploit

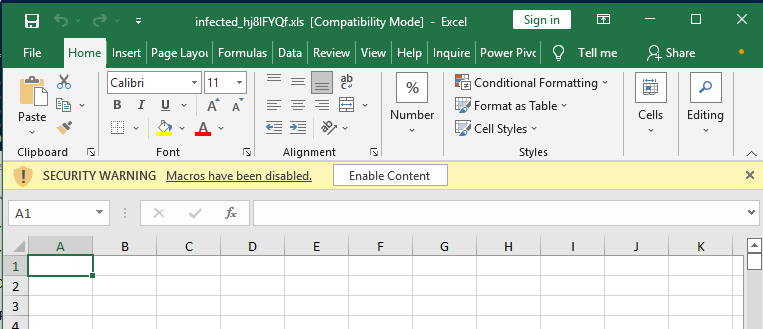


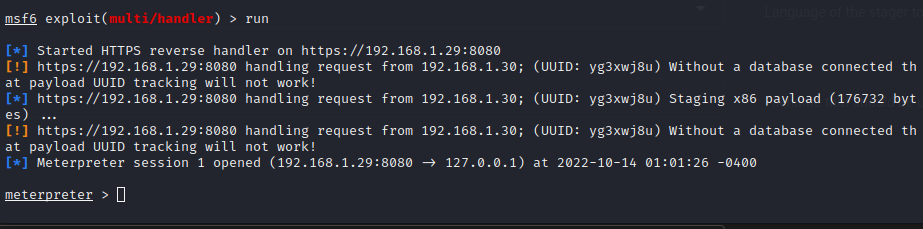












POWERSHELL EMPIRE

