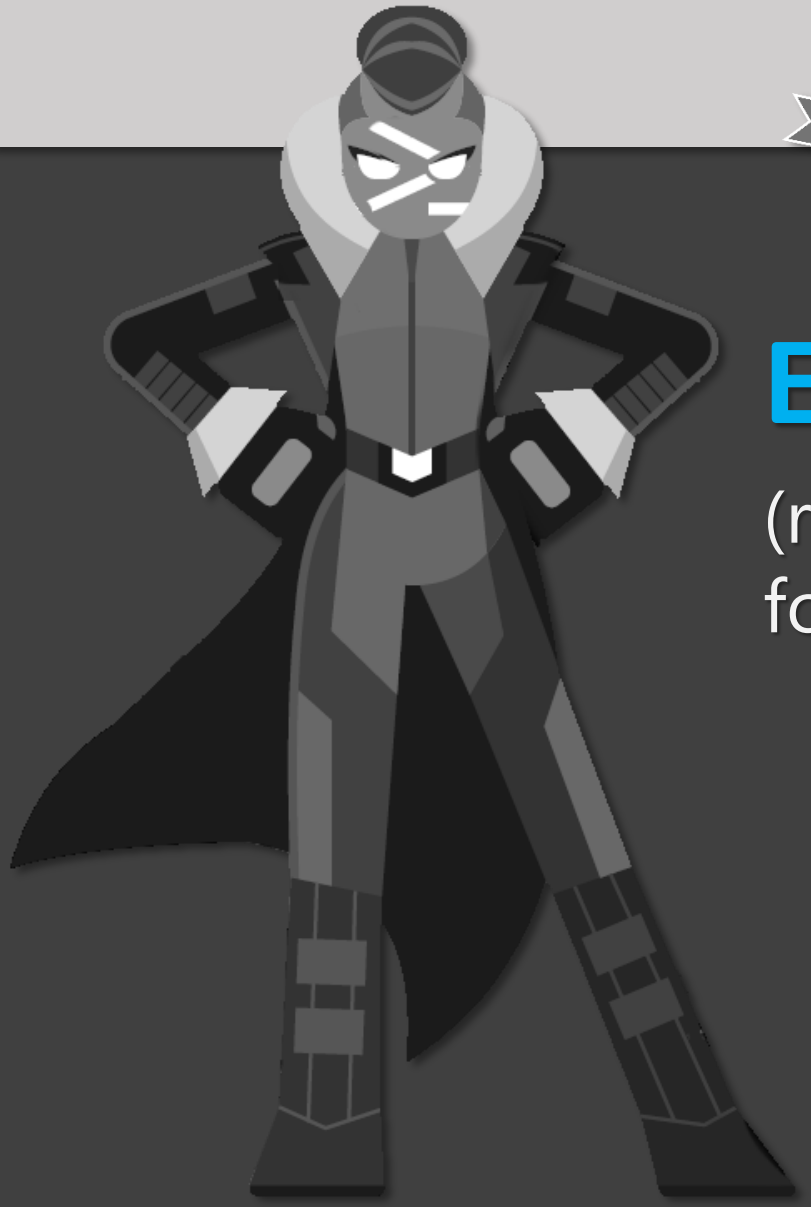
PSCONF.EU



PSCONF.EU

2018

Empire Strikes Back

(re)Building a PowerShell Module for Empire Automation

Walter Legoswki aka @SadProcessor

Agenda

I - What is Empire?

II - What is EmpireStrike?

III - What is next…

Whois/Disclaimer

n00b

PSCONF.EU

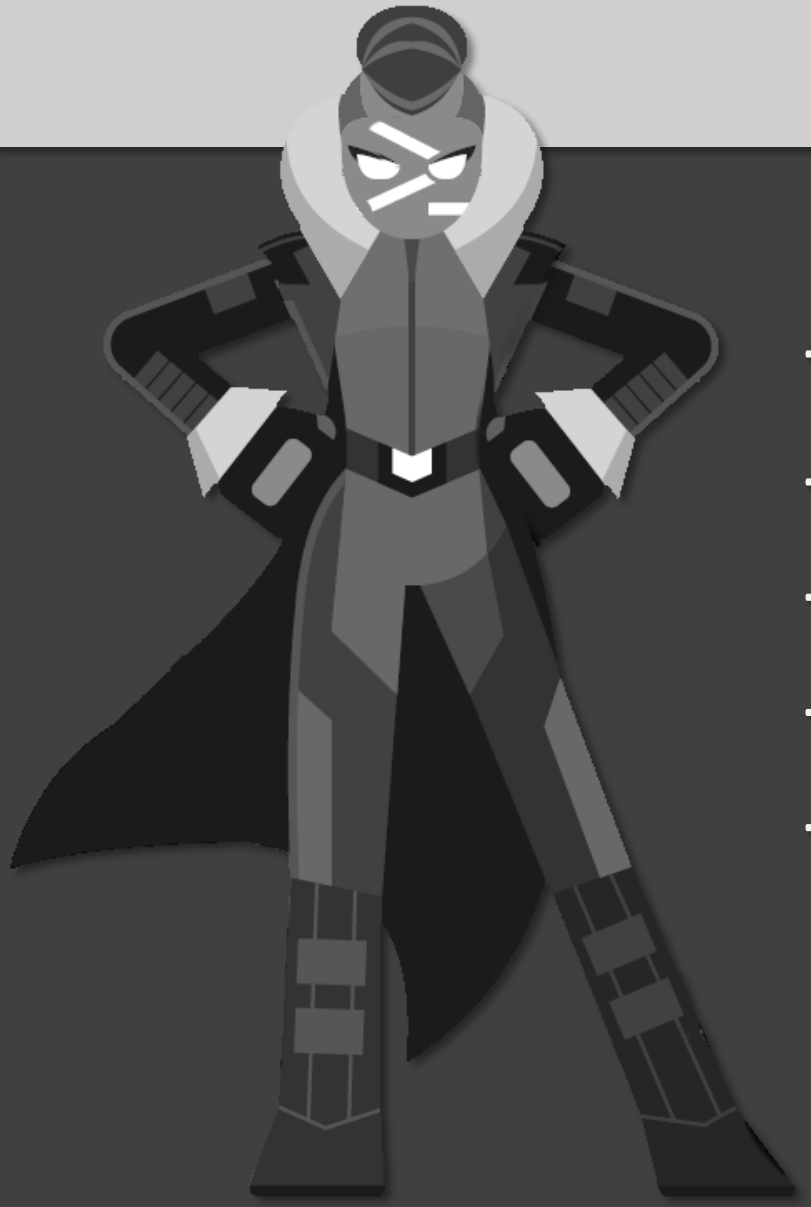
Whois/Disclaimer

n00b

Whois/Disclaimer

n00b

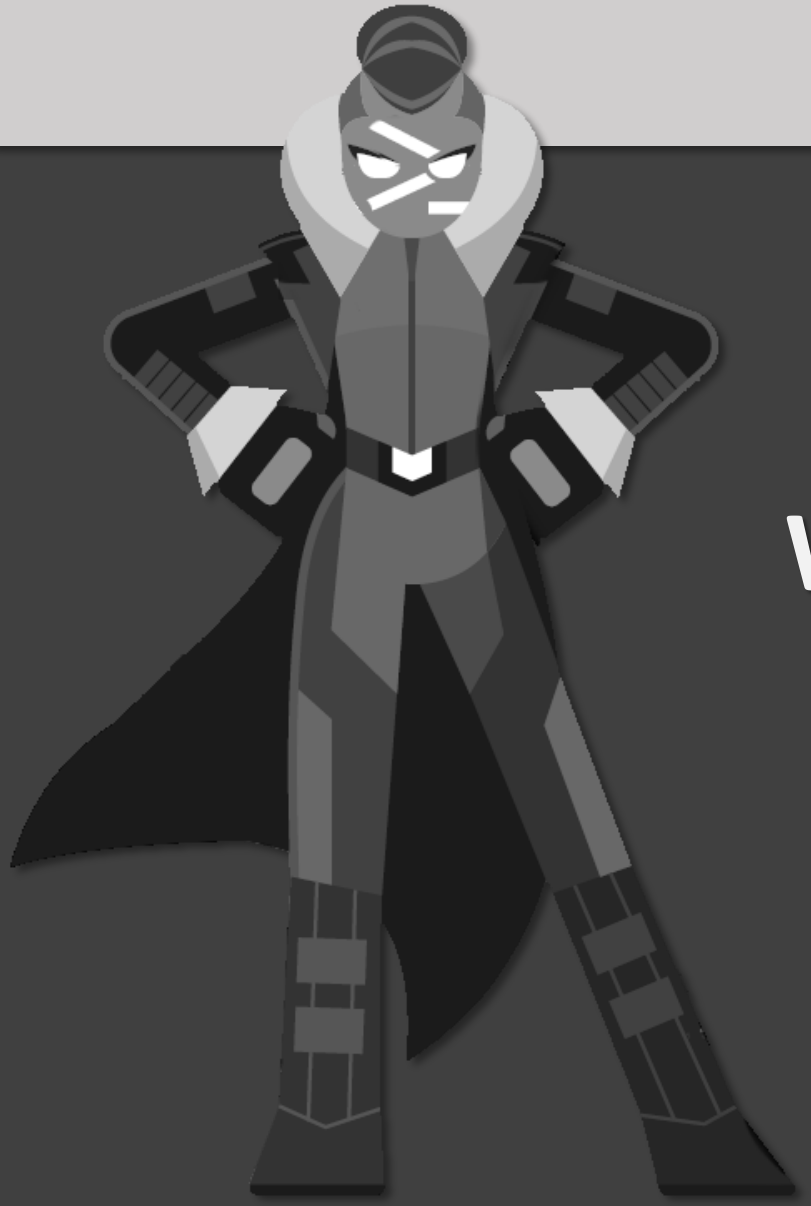
Goal



- Share **Passion**
- Share **Ideas**
- Share **Tools**
- Share **Joys & Pains**
- Share **Tips & Tricks**

(take home what you like…)

Part I



What is Empire ?

Empire – Credits

@harmj0y
@sixdub
@enigma0x3
@killswitch_gui
@xorrior
@424f424f
aka rvrsh3ll

Empire – Credits

@harmj0y
@sixdub
@enigma0x3
@killswitch_gui
@xorrior
@424f424f
aka rvrsh3ll

+ **Contribs.**
+ **Maintainers**
  @xorrior
  @mr64Bit
  @Dakota_Nelson
  & more...

Empire – Definition

Empire is a post-exploitation framework that includes a pure-PowerShell2.0 Windows agent, and a pure Python 2.6/2.7 Linux/OS X agent. It is the merge of the previous PowerShell Empire and Python EmPyre projects. The framework offers cryptologically-secure communications and a flexible architecture. On the PowerShell side, Empire implements the ability to run PowerShell agents without needing powershell.exe, rapidly deployable post-exploitation modules ranging from key loggers to Mimikatz, and adaptable communications to evade network detection, all wrapped up in a usability-focused framework

src: Empire Wiki

Empire – Definition

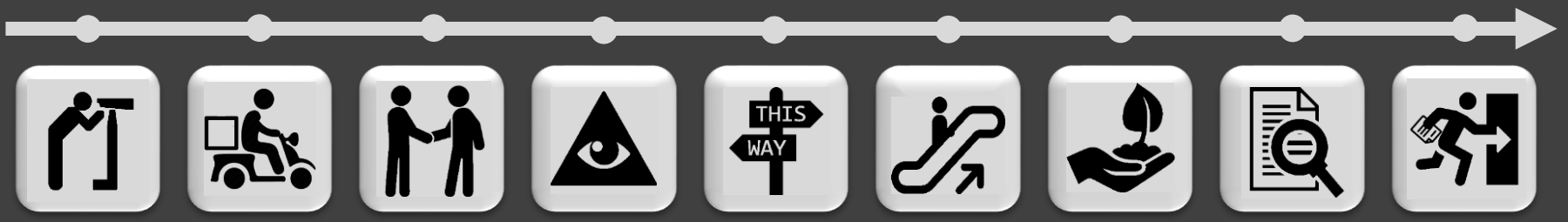
Empire is a **post-exploitation framework** that includes a pure-**PowerShell** 2.0 **Windows** agent, and a pure **Python** 2.6/2.7 **Linux/OS X** agent. It is the merge of the previous PowerShell Empire and Python EmPyre projects. The framework offers cryptologically-secure communications and a flexible architecture. On the PowerShell side, Empire implements the ability to run PowerShell agents **without needing powershell.exe**, rapidly deployable post-exploitation modules ranging from **key loggers** to **Mimikatz**, and **adaptable communications** to evade network detection, all wrapped up in a **usability-focused framework**

PSCONF.EU

Empire – Definition

Empire is a **post-exploitation framework** that includes a pure-PowerShell2.0 Windows agent, and a pure Python 2.6/2.7 Linux/OS X agent. It is the merge of the previous PowerShell Empire and Python EmPyre projects. The framework offers cryptologically-secure communications and a flexible architecture. On the PowerShell side, Empire implements the ability to run PowerShell agents without needing powershell.exe, rapidly deployable post-exploitation modules ranging from key loggers to Mimikatz, and adaptable communications to evade network detection, all wrapped up in a usability-focused framework

Attacker Kill Chain



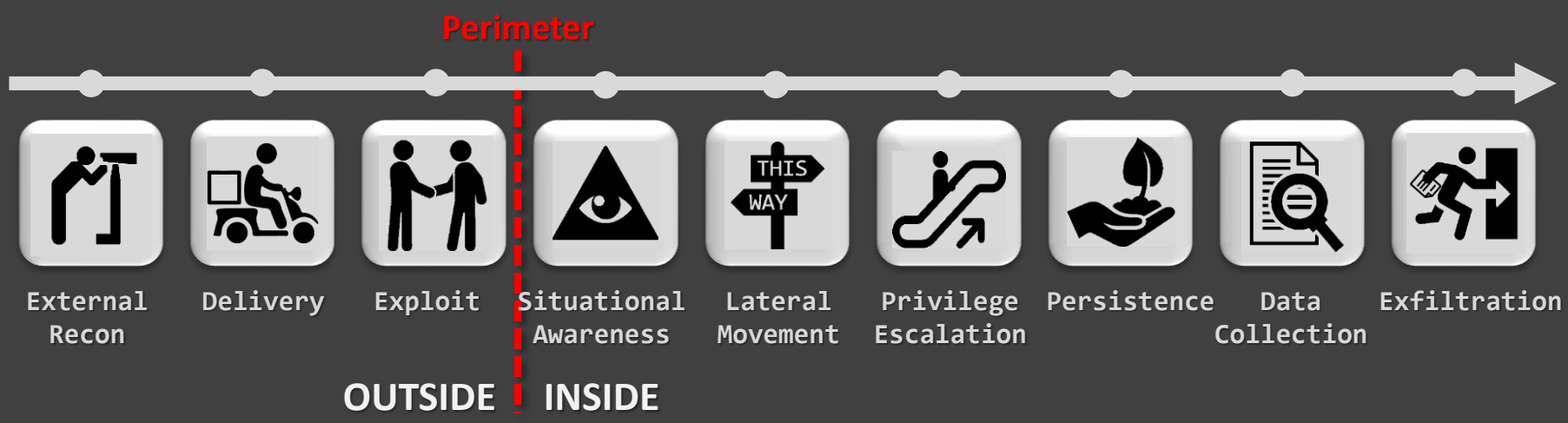
External Recon | Delivery | Exploit | Situational Awareness | Lateral Movement | Privilege Escalation | Persistence | Data Collection | Exfiltration

Attacker Kill Chain

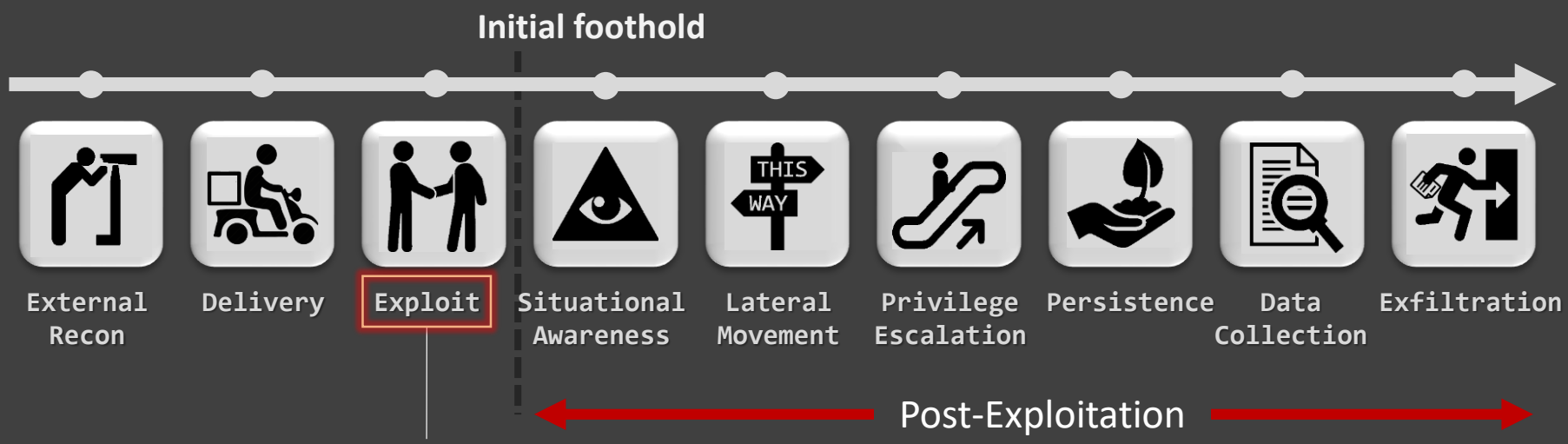
Taxonomy of:

- Actions attacker needs to take to achieve goal
- Opportunities for defenders to catch attackers while in action…

Attacker Kill Chain

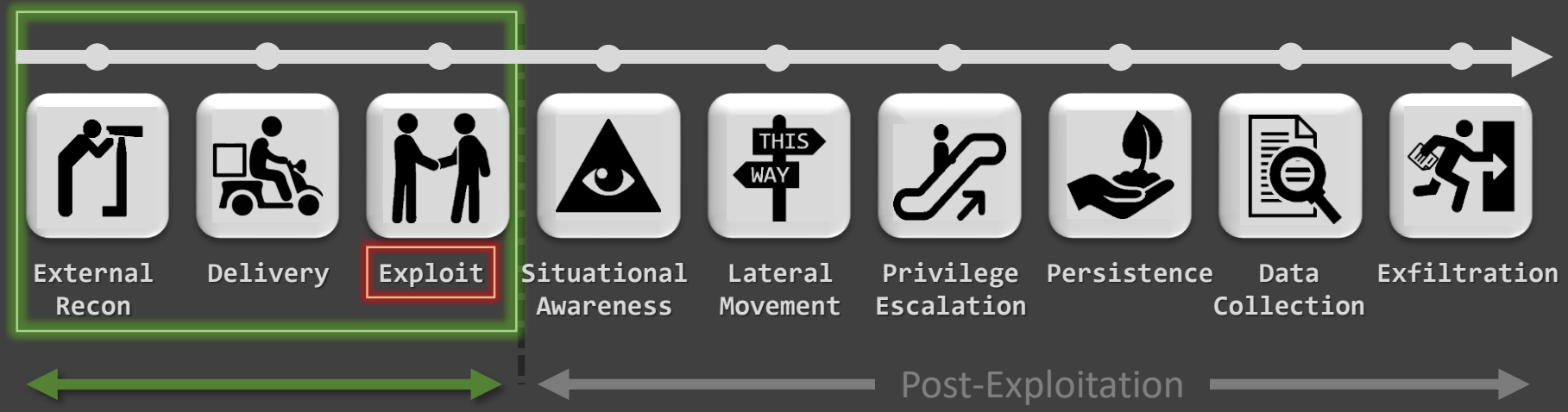


Attacker Kill Chain



0-Day
WebApps
Configs/Patchs
Insiders
Leaked Creds
Phishing
& more...

Basic Defense



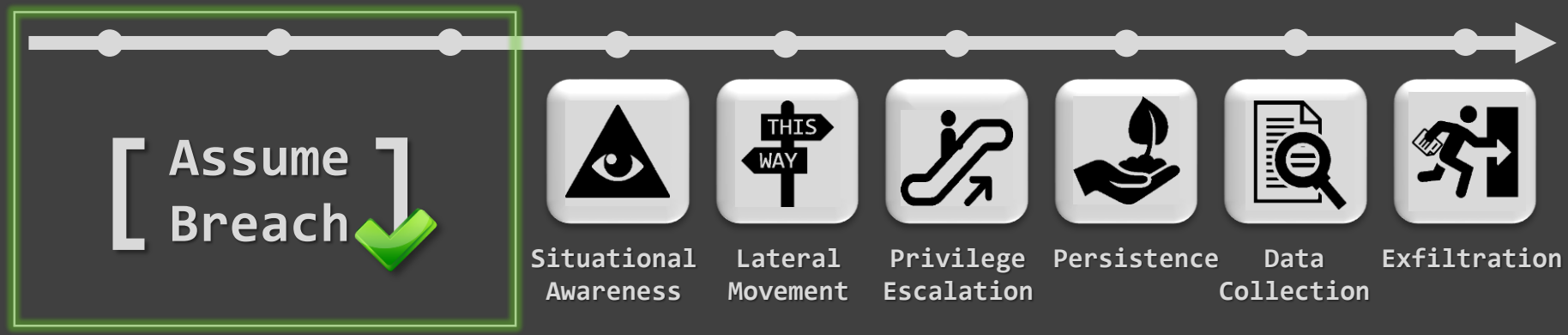
Focus:
- Avoid Exploit
- Perimeter Defenses

The Idea

~~The Idea~~

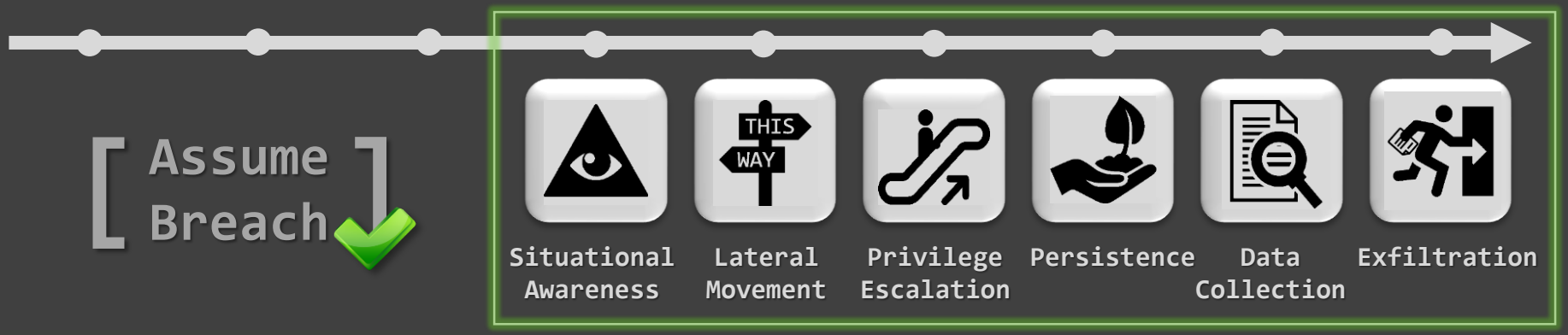
~~The Idea~~

The Idea – Defense In Depth



The Idea – Defense In Depth

[Assume Breach]



RedTeam vs BlueTeam

Adversary Simulation & Threat Hunting

What is Empire?

What is Empire?

Post-Exploitation Framework

RedTeam / Adversary Simulation

What is Empire?

Post-Exploitation Framework

RedTeam / Adversary Simulation

"An open-source <u>toolset made to replicate adversary actions</u> in your internal network"

Empire – Terminology

Empire – Terminology

Listener:

- **Listens for his set of Agents**
- **Receives Results**
- **Various communication profiles**

Empire – Terminology

Stager:

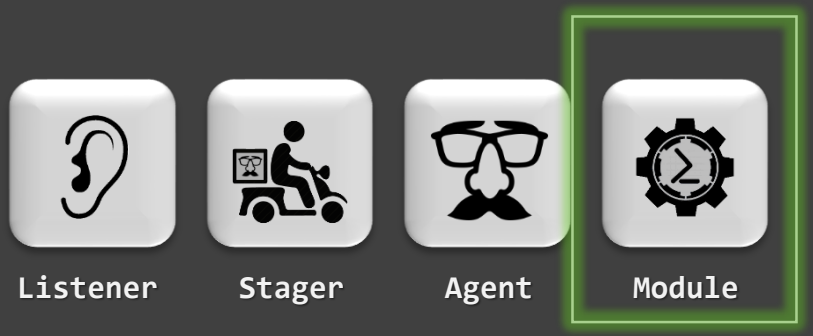
- **Delivers Agent to Target**
- **Various formats/methods**

Empire – Terminology

Agent:

- Calls Listener at regular interval
- Asks if any tasks for him
- Executes and sends result
- Runs in memory

Empire – Terminology



Module:

- PowerShell (+Python) Scripts (284)
- Tasked to Agent for Execution
- Result sent back to Listener

PSCONF.EU

Empire – Action

Bad Guy

Target

Empire – Action

Setup a Listener

[Listener type determines Agent communication profile]

Empire – Action

Generate a Stager for that Listener type

[Stager type depends on Agent delivery/launch method]

Empire – Action

Deliver to Target

Empire – Action

Agent Checks in

Empire – Action

PSCONF.EU

Empire – Action

“ Do you have anything for me ? ”

Empire – Action

[Sleep]

Empire – Action

“ Do you have anything for me ? ”

Empire – Action

[Sleep]

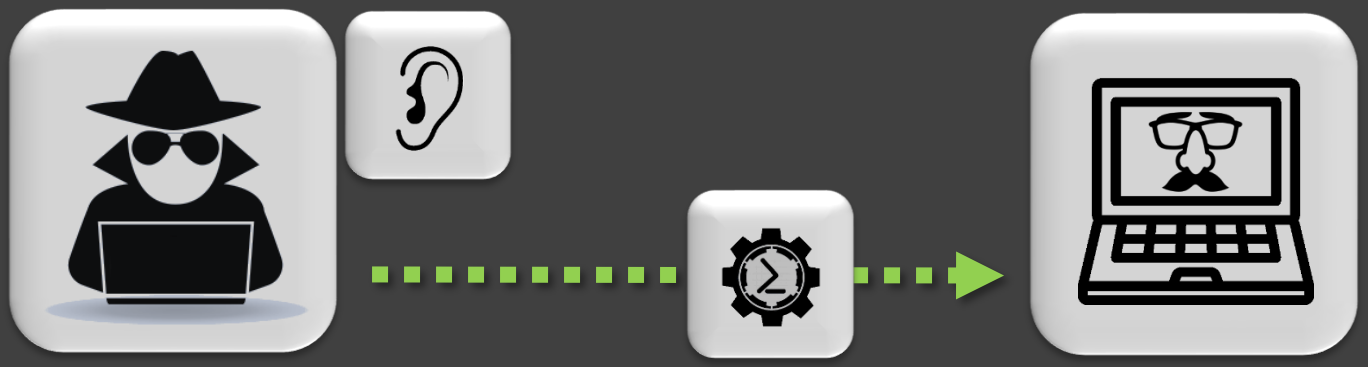
Empire – Action

Module tasked to Agent buffer

Empire – Action

“ Do you have anything for me ? ”

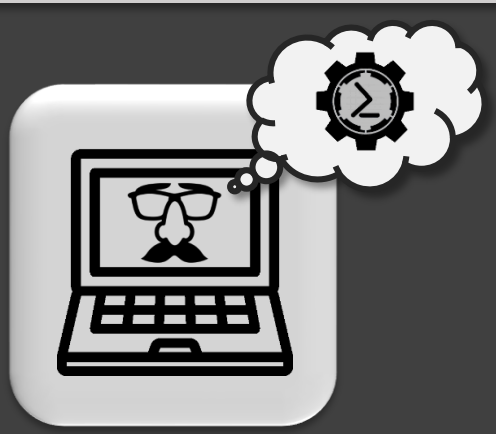
Empire – Action



Module sent to Agent

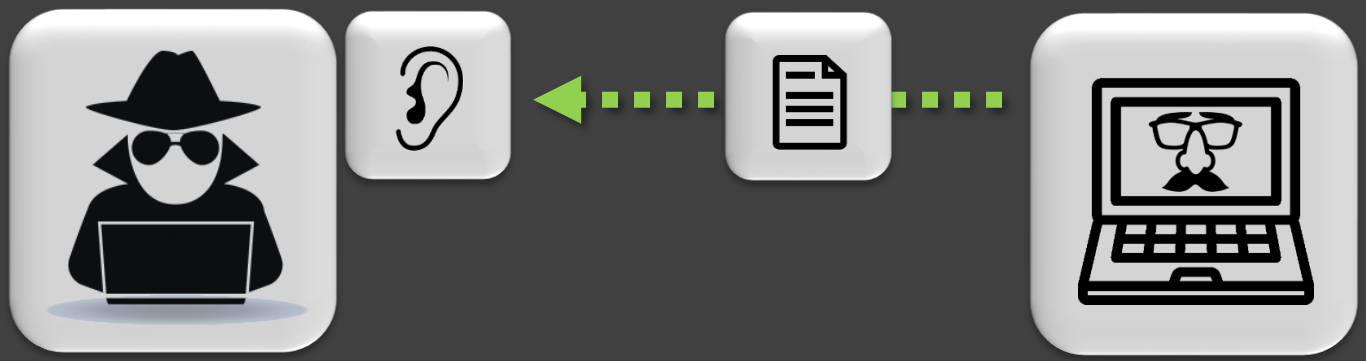
PSCONF.EU

Empire – Action



Module executed by Agent

Empire – Action



Results sent back to Listener

Empire – Action

Voila!

Empire – Action

and so on… and so on…

Empire – Action

and so on… and so on…

Empire – Look & Feel

```
>_
=================================================================
 [Empire]  Post-Exploitation Framework
=================================================================
 [Version] 2.5 | [Web] https://github.com/empireProject/Empire
=================================================================

  _______ .___  ___. .______    __  .______       _______
 |   ____||   \/   | |   _  \  |  | |   _  \     |   ____|
 |  |__   |  \  /  | |  |_)  | |  | |  |_)  |    |  |__
 |   __|  |  |\/|  | |   ___/  |  | |      /     |   __|
 |  |____ |  |  |  | |  |      |  | |  |\  \----.|  |____
 |_______||__|  |__| | _|      |__| | _| `._____||_______|


       284 modules currently loaded

       1 listeners currently active

       1 agents currently active


(Empire) >
```

Questions?

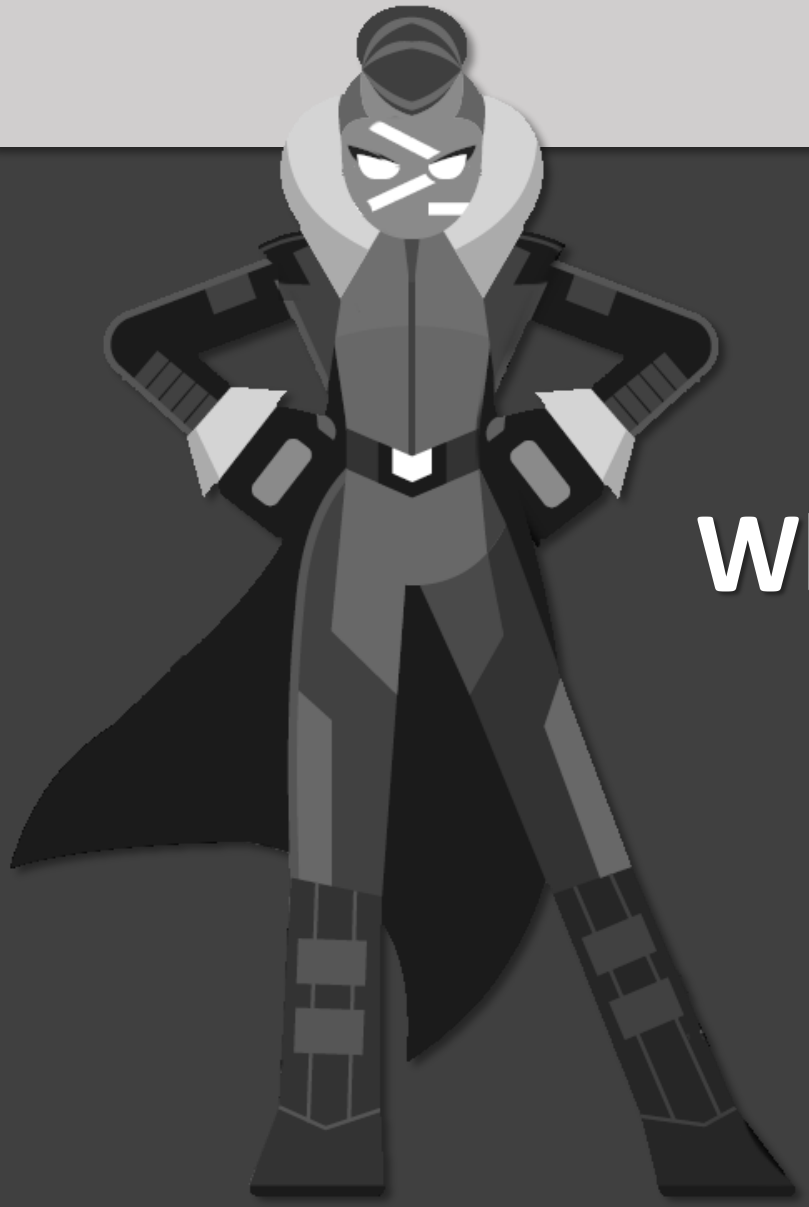
?

Write-EmpireModule

Demo

ISE DEMO – WRITE-EMPIREMODULE

Part II



What is EmpireStrike ?

EmpireStrike - Definition

EmpireStrike - Cmdlets

```
Cmdlet          Synopsis                          Help
------          --------                          ----
Empire-Admin    Empire Admin Stuff                Help Admin
Empire-Agent    Interact with Empire Agents       Help Agent
Empire-Cred     Interact with Empire Cred DB      Help Cred
Empire-Event    View Empire Events                Help Event
Empire-Exec     Execute Commands on agent         Help Exec
Empire-Help     View EmpireStrike Cheat Sheet     Help Empire
Empire-Listener Interact with Empire Listeners    Help Listener
Empire-Module   Interact with Empire Modules      Help Mod
Empire-Option   Set Module Options                Help Option
Empire-Result   Get Agent result                  Help Result
Empire-Search   Empire Module Search              Help Search
Empire-Session  Interact with Empire Sessions     Help Session
Empire-Sniper   Shoot from Scriptpane (ISE/VSCode) Help Sniper
Empire-Speak    Add Voice to Automations          Help Speak
Empire-Stager   Interact with Empire Stagers      Help Stager
Empire-Strike   Execute Empire Modules            Help Strike
Empire-Sync     Sync Empire Objects               Help Sync
Empire-Target   View/Set Target                   Help Target
Empire-Tune     Play Imperial March               Help Tune
Empire-Use      Select Stager|Listener|Module     Help Use
Empire-View     View Empire Objects               Help View
```

EmpireStrike - Cmdlets

```
Cmdlet          Synopsis                          Help
------          --------                          ----
Empire-Admin    Empire Admin Stuff                Help Admin
Empire-Agent    Interact with Empire Agents       Help Agent
Empire-Cred     Interact with Empire Cred DB      Help Cred
Empire-Event    View Empire Events                Help Event
Empire-Exec     Execute Commands on agent         Help Exec

Empire-Listener Interact with Empire Listeners    Help Listener
Empire-Module   Interact with Empire Modules      Help Mod
Empire-Option   Set Module Options                Help Option
Empire-Result   Get Agent result                  Help Result

Empire-Session  Interact with Empire Sessions     Help Session


Empire-Stager   Interact with Empire Stagers      Help Stager
Empire-Strike   Execute Empire Modules            Help Strike
```

EmpireStrike - Cmdlets

```
Admin    Empire Admin Stuff
Agent    Interact with Empire Agents
Cred     Interact with Empire Cred DB
Event    View Empire Events
Exec     Execute Commands on agent

Listener Interact with Empire Listeners
Modul    Interact with Empire Modules
Option   Set Module Options
Result   Get Agent result

Session  Interact with Empire Sessions


Stager   Interact with Empire Stagers
Strike   Execute Empire Modules
```

EmpireStrike – Design

EmpireStrike – Features

- Short Syntax (+Redundancy)
- Aliases Galore
- Tab-Completion
- Dynamic Params
- Return Objects
- Pipeline Input
- Multiple Sessions

Think
Ty<TAB>
Get

ISE DEMO – EMPIRESTRIKE CMDLETS

VIDEO DEMO – EMPIRESTRIKE AUTOMATION

https://youtu.be/BbjeC28dA9s?list=PLdhDuST3OlrNRull1hITtWVYzIQPfWjXD

What next?

What next…

What next…

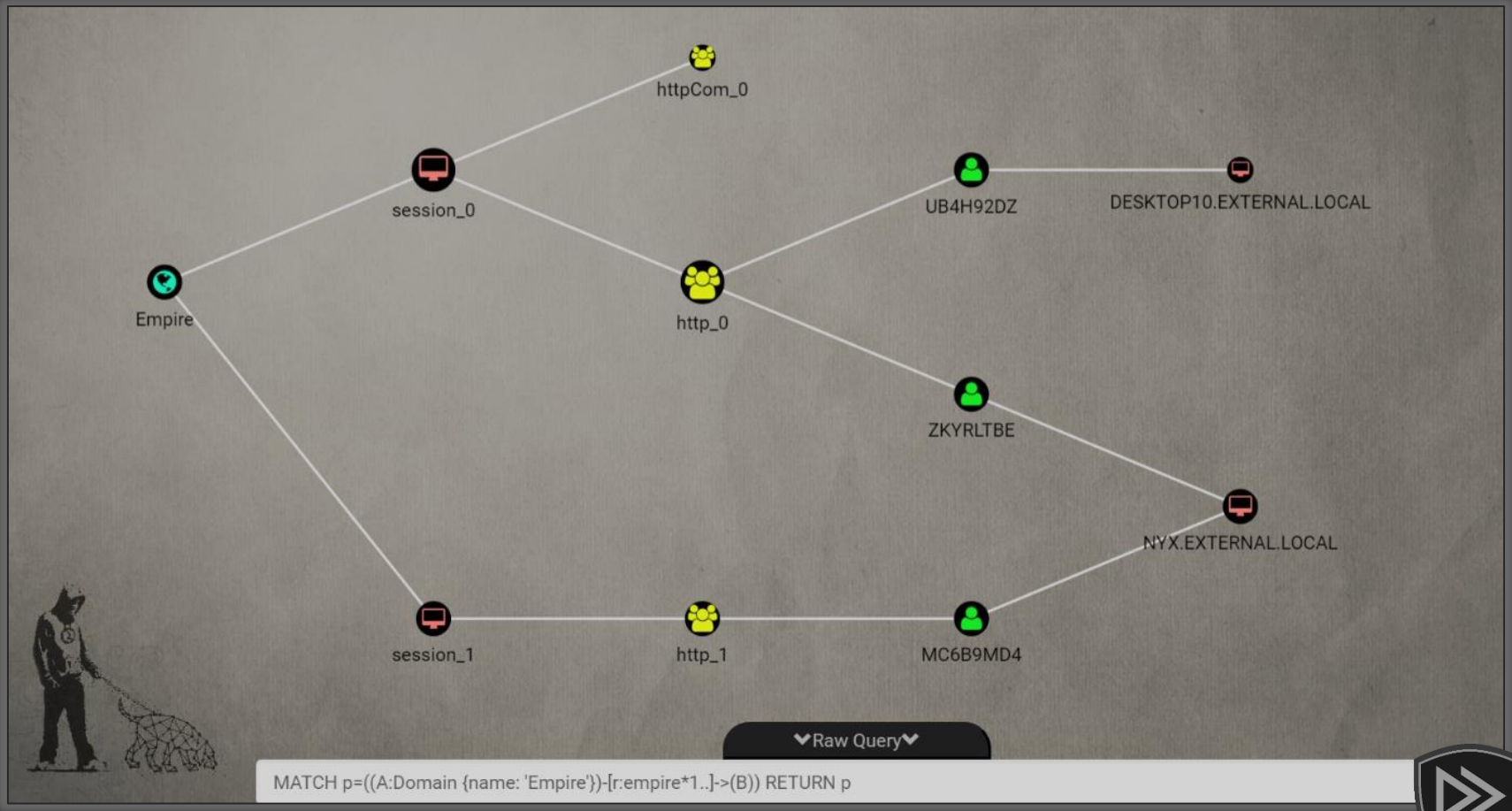
You:

- Download **EmpireStrike** and play with it
- Use EmpireStrike for **live** Red Team **action**
- Write **automations** for recurring offensive routines
- Add **new features** to make it better

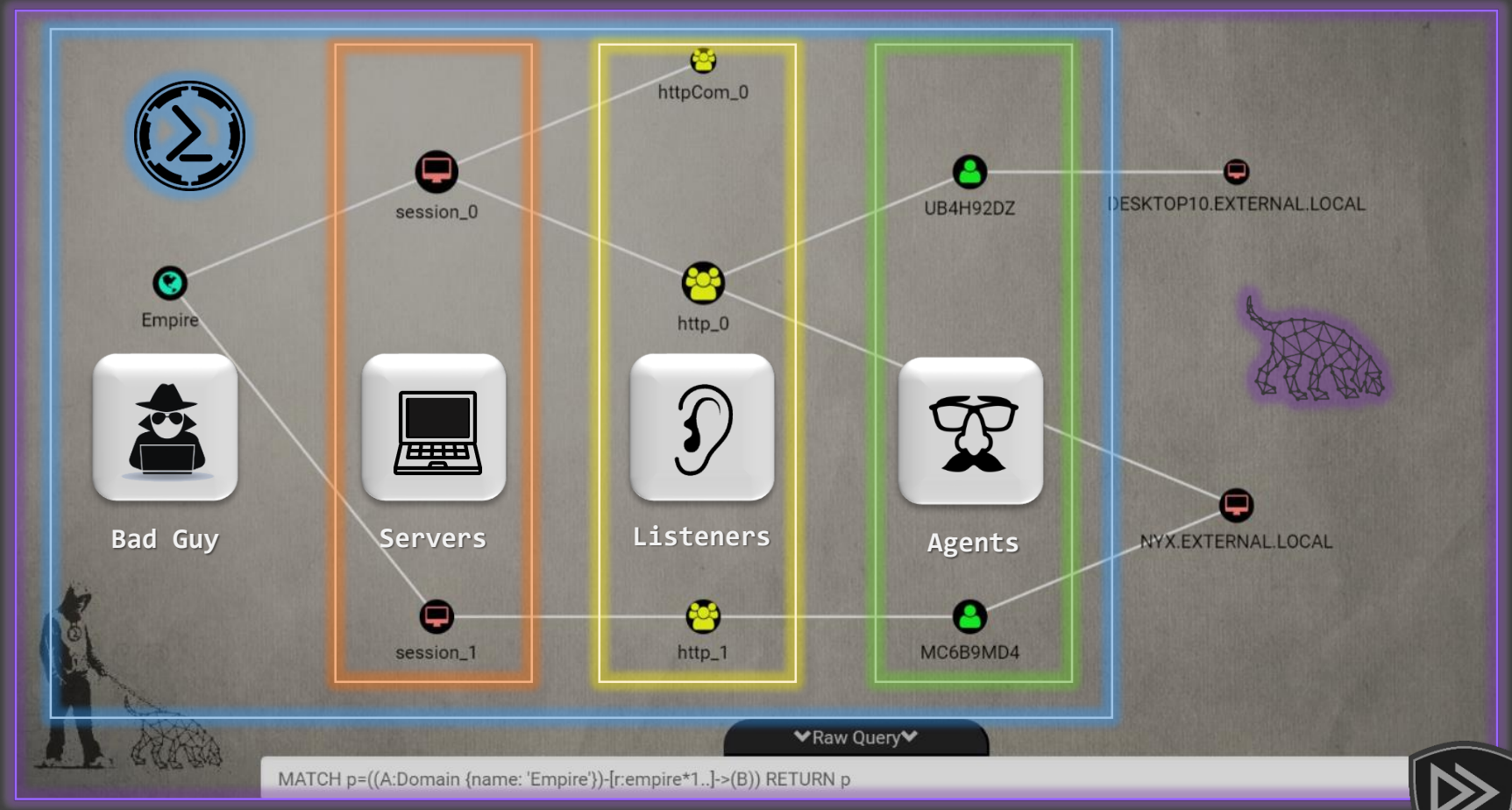
Me:

- Merge **Empire & BloodHound** (+ATT&CK)

What next…


httpCom_0
session_0
UB4H92DZ
DESKTOP10.EXTERNAL.LOCAL
Empire
http_0
ZKYRLTBE
NYX.EXTERNAL.LOCAL
session_1
http_1
MC6B9MD4
Raw Query
MATCH p=((A:Domain {name: 'Empire'})-[r:empire*1..]->(B)) RETURN p

What next…


httpCom_0
session_0
UB4H92DZ
DESKTOP10.EXTERNAL.LOCAL
Empire
http_0
Bad Guy
Servers
Listeners
Agents
NYX.EXTERNAL.LOCAL
session_1
http_1
MC6B9MD4
Raw Query
MATCH p=((A:Domain {name: 'Empire'})-[r:empire*1..]->(B)) RETURN p

Questions?

More Info – Empire

- Empire Source:
  https://github.com/EmpireProject/Empire
- Empire Wiki:
  https://github.com/EmpireProject/Empire/wiki
- Empire Slack:
  https://adaptiveempire.slack.com

- EmpireStrikeX:
  https://github.com/sadprocessor/SomeStuff/EmpireStrikeX

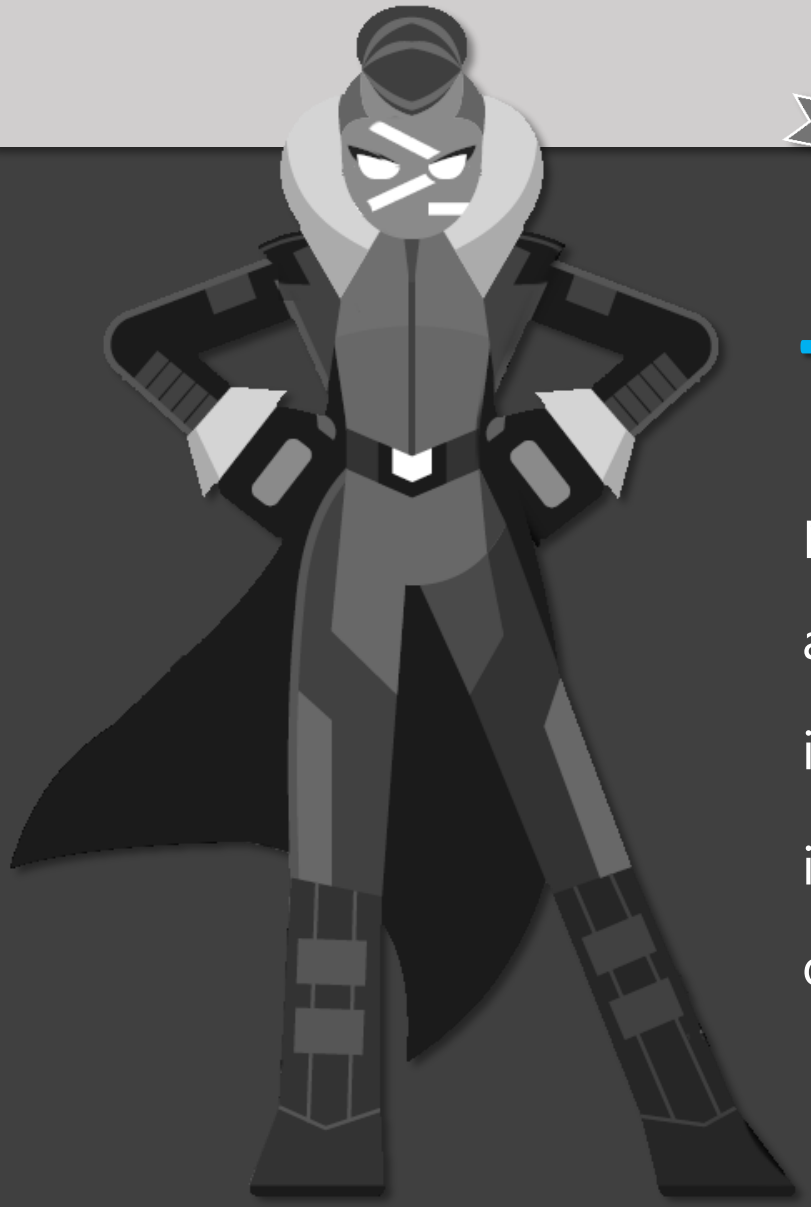
Summary

- PowerShell **Empire is really awesome**
- EmpireStrike makes it even better

- Tool-Making with **PowerShell is really awesome**
- If this guy can do it, so can I… (Make it so!)

- **PSConfEU is really awesome !!**

Summary



PSCONF.EU

2018

Thank you

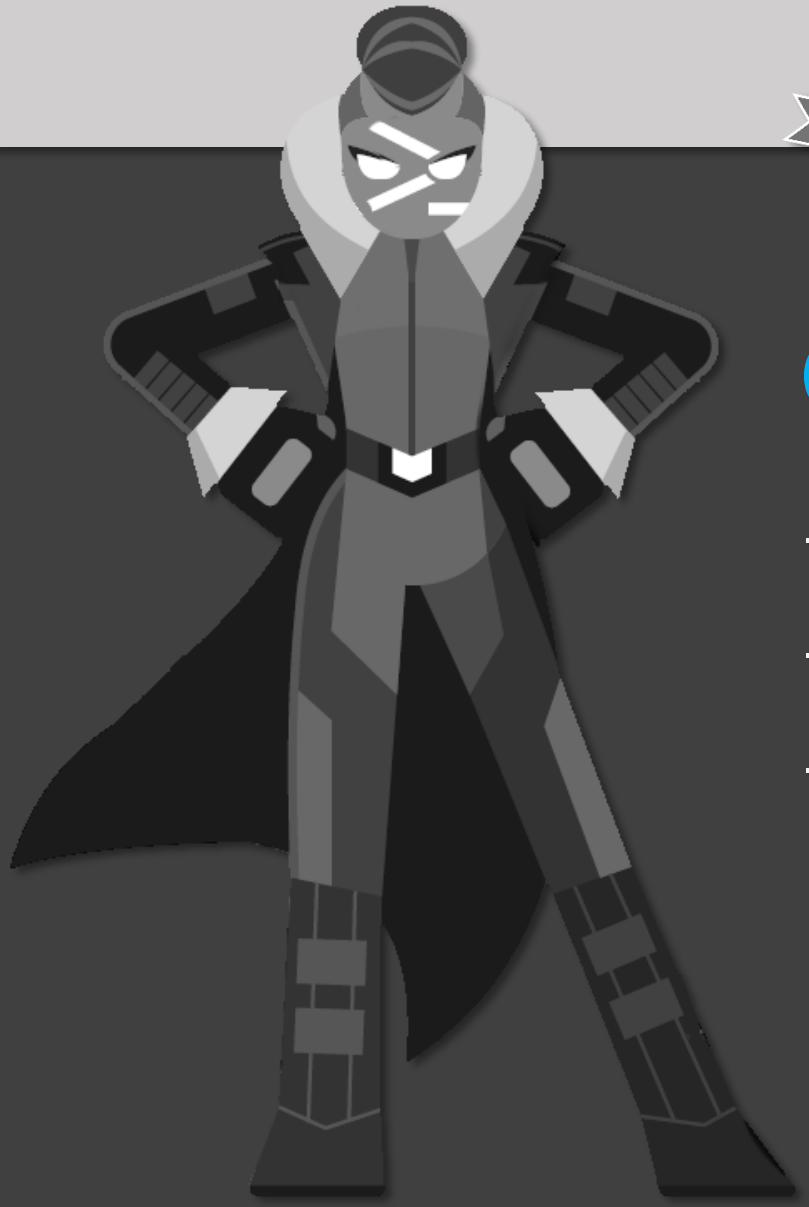
Meetup in the **breakout room**

after this session

if you have **more questions**

if you want to **test this tool**

or simply for a drink...



Now…

2018

Get-Break -Min 15

- Grab a coffee / Have a Chat
- Change Room/Track
- Stay here for next talk

Enjoy **PSConfEU 2018**…

PSCONF.EU