Meeting Starts at 6:05PM

OWASP Sacramento

Ryan Kozak

August 2021

Agenda

1) Community Topics
    - Call for Presentations
    - OWASP Slack
2) Empire Framework Introduction
3) Empire Demo

OWASP Community

Call for Presentations: **September** and **October** (likely virtual events)

If you'd like to present (or know someone else who would) at the OWASP Sacramento Chapter's September or October meetings, please email us your topic.

You don't need to be an expert!

Joubin: joubin.jabbari@owasp.org
Ryan: ryan.kozak@owasp.org

OWASP Community

OWASP Slack

- https://bit.ly/3ckwNfI
- Or go to our Chapter page: OWASP Sacramento CA Local Chapter Meetup | OWASP Foundation

Empire

Disclaimers

1. I’m not an expert on this tool.

2. Don’t use this tool to do bad stuff.

Post-Exploitation Framework

What is Empire?

Empire 4 is a post-exploitation framework that includes a pure-PowerShell Windows agents, Python 3.x Linux/OS X agents, and C# agents.

It is the merger of the previous PowerShell Empire and Python EmPyre projects.

Original Developers: @harmj0y,@sixdub, and @enigma0x3

Currently Maintained by BC Security

Post-Exploitation Framework

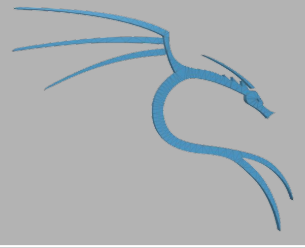
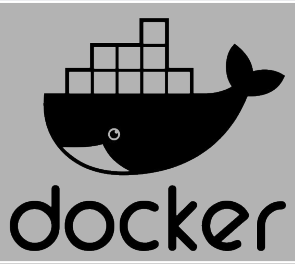
Who is Empire for?

- Red Teams
- Penetration Testers
- Purple Teams
- The Curious...

Empire “Components”

- **Listeners**
  - Similar to Metasploit’s multi/handler, listens for incoming connections.
- **Stagers**
  - Code executed on victim machine which connects back to a listener.
- **Agents**
  - The final payload retrieved by the stager...running on a victim machine under control of the C2 server.
- **Modules**
  - True power of Empire, easily run code for situational awareness, credentials and privilege escalation, lateral movement, trolling, etc.
- **Plugins**
  - Custom scripts to add functionality.
- **Interfaces**
  - Starkiller (uses API), REST API, and Command Line

Empire Installation

`sudo apt install powershell-empire`	`docker pull bcsecurity/empire:latest`
	
	`docker create -v /empire --name data bcsecurity/empire:latest`
	
	`docker run -it -p 1337:1337 -p 5000:5000 --volumes-from data bcsecurity/empire:latest`
		`sudo pip3 install poetry`
		
		`git clone --recursive https://github.com/BC-SECURITY/Empire.git`
		
		`cd Empire`
		
		`sudo ./setup/install.sh`
		
		`sudo poetry install`

Demo

Duration – 30 min(ish)

Conclusion

- Empire is a great post exploitation framework and C2 server
- Built for attackers, defenders, researchers, and so on.
- Many options to create listeners (http, Dropbox, OneDrive, etc).
- Many options to create stagers (a whole lot).
- Modules are Powershell, Python 3.x, or C#.
- Modules for persistence, privilege escalation, credential harvesting, situational awareness, trolling, data collection, etc.

References

- https://github.com/BC-SECURITY/Empire
- https://github.com/BC-SECURITY/Starkiller