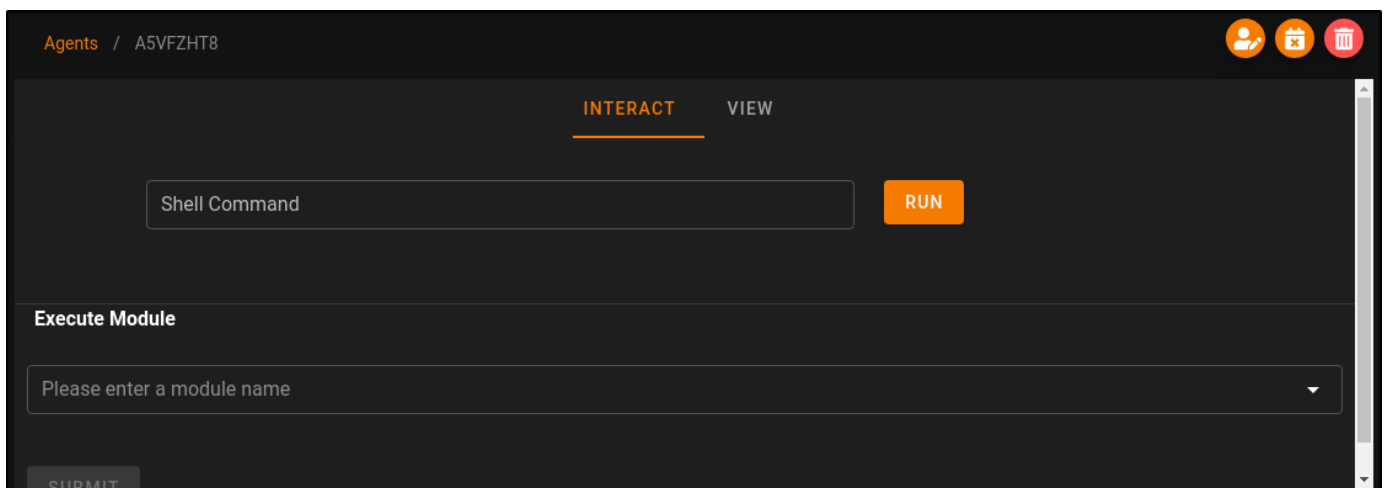# 17

Now that we have an agent on the machine responding with Starkiller we can explore the command interface of Starkiller as well as the modules that Starkiller has.

Agent Panel Overview

If you click on an agent you will be brought to the agent interaction panel, here you can send commands to the server as well as execute modules within Starkiller.

Agent interaction menu

The agent can send any normal shell commands such as whoami or ls, however that is not utilizing the full power of Starkiller.

Starkiller Modules Overview
One of the major features of any c2 server is the ability to use modules. These are typically tools or exploits like mimikatz, Rubeus, and printspoofer that can be loaded onto the server through the agent.

	Name	Language	Minimum Language Version	Needs Admin	Opsec Safe	Background	Techniques	Actions
⌄	exfiltration/Invoke_ExfilDataToGitHub	powershell	3	false	true	false		▶
⌄	external/generate_agent	Python		false	true	true		▶
⌄	python/privesc/osx/dyld_print_to_file	python	2.6	false	false	false	TA0004	▶
⌄	python/privesc/osx/piggyback	python	2.6	false	false	false	T1050	▶

Starkiller module menu

Starkiller has many modules, all their own uses. Take some time to explore the modules menu and play with some of the modules.

Starkiller Credentials and Reporting Overview
Starkiller is great for saving information and logging actions because it will automatically save all credentials that are found through the modules or credentials that you add manually. Starkiller will also report all shell command and modules run on an agent.

id	CredType	Username	Password	Domain	Host	Notes	SID
1	hash	user 🔗	password 🔗	EXAMPLE.local	EXAMPLE-WS01		

Starkiller credentials panel

	Agent	Task ID	Event Type	Task Command	User	Timestamp
⌄	CZ75FRSB	3	task	ls	empireadmin	4 hours ago
⌄	CZ75FRSB	2	task	whoami	empireadmin	4 hours ago
⌄	CZ75FRSB	1	task	whoami	empireadmin	4 hours ago
⌄	CZ75FRSB		checkin			4 hours ago

Starkiller reporting panel

Answer the questions below

Read the above text and familiarize yourself with the menus.

Question Done