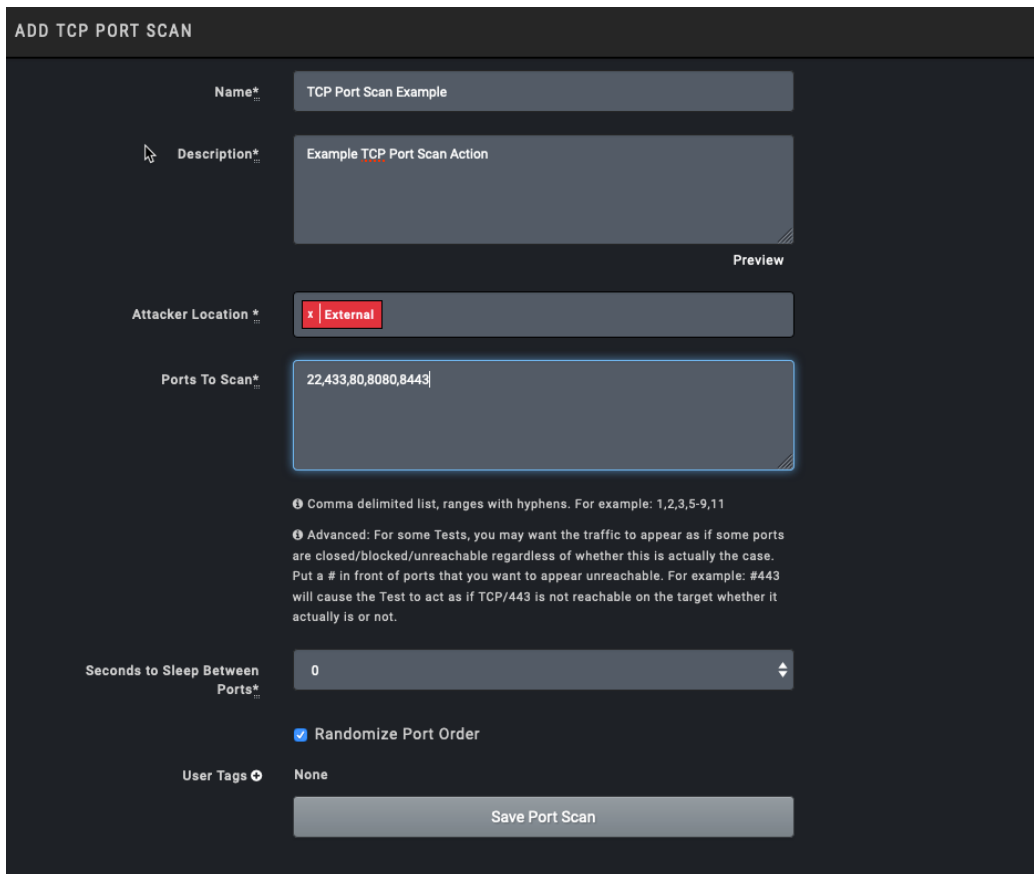


ADDING TCP PORT SCAN ACTIONS

TCP Port Scan Actions are typically used to validate network segmentation or to simulate typical reconnaissance activities like full port scans and services fingerprinting.

1. Within the Director, click on **Library > Actions** in the top navigation bar.
2. Click **Add Action** and select **TCP Port Scan**. The Add TCP Action form displays.
3. Populate the Form.
 - a. Name
 - b. Description
 - c. Attacker location
 - d. Ports to be scanned
 - Separate multiple entries with commas
 - Ranges: use a dash (-) in between the first and last port
 - Ports that should show as closed/unreachable: Add a pound sign (#) in front of the port number
 - e. Seconds to Sleep between Ports
 - f. (Optional) Select **Randomize Port Order**.
4. Click **Save Port Scan**.

The Action Library displays. A confirmation message that your Action was created successfully is shown and the Action is selected and displayed in the Action preview.



ADD TCP PORT SCAN

Name* TCP Port Scan Example

Description* Example TCP Port Scan Action

Attacker Location * External

Ports To Scan* 22,433,80,8080,8443

Comma delimited list, ranges with hyphens. For example: 1,2,3,5-9,11

Advanced: For some Tests, you may want the traffic to appear as if some ports are closed/blocked/unreachable regardless of whether this is actually the case. Put a # in front of ports that you want to appear unreachable. For example: #443 will cause the Test to act as if TCP/443 is not reachable on the target whether it actually is or not.

Seconds to Sleep Between Ports* 0

Randomize Port Order

User Tags None

Save Port Scan

Adding a TCP Port Scan Action



When a TCP port scan cannot reach out on ports configured in the Actor Communication settings, the map reflects no communication. This is likely from a firewall or device recognizing the behavior and preventing it.