TP ACTION MANAGER

Diateam

- Présentation Action Manager
- Installation & utilisation sous Linux
- Création d'une action simple
- Installation & utilisation sous Windows
- Création d'une action complexe
- Aller plus loin via l'API

ACTION MANAGER

Quoi ?

- Agents capable d'exécuter des « actions » (Windows GNU/Linux) connectés via un port série
- Un service pour les gouverner tous
- Une API afin de pouvoir donner des ordres à ces agents
- Une interface WEB intuitive permettant d'utiliser l'API de façon simple

ACTION MANAGER

Pourquoi ?

- Génération de trafic de vie, création/lecture/écriture de fichiers, communication
- Automatisation de taches
- Automatisation de scénarios complexes en enchainant des actions
- Et plus !

Vérification

On veut vérifier automatiquement qu'on a bien réussi à neutraliser l'agent tooters dans notre LAN. On va donc installer l'action manager dans la machine wireshark.

INSTALLATION

3 fichiers

- `stub_linux-amd64` : Le binaire qui va télécharger l'agent réel
- `config.yaml` : La configuration du stub (ne change jamais, optionnel dans le futur)
- `am-stub.service` : Un service systemd afin de pouvoir automatiquement lancer l'agent au démarrage.

Ces fichiers peuvent être retrouvés sur le master dans `/usr/share/actionmanager/agent_stubs/`

INSTALLATION

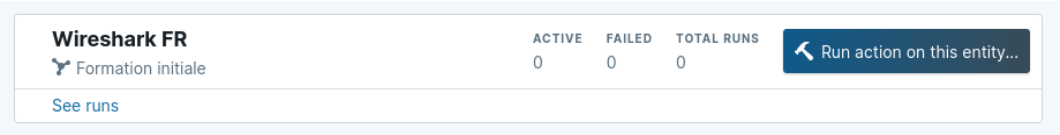
Sur la machine wireshark :

- Désinstancier la machine, ouvrir ses options
- Dans l'onglet hynesim, cocher l'option du port série pour l'action manager
- Allumer la machine
- Créer un dossier `/opt/hns-actionmanager`
- Mettre le stub et sa configuration dans ce dossier
- Copier le service dans le dossier `/etc/systemd/system/`
- Lancer la commande suivante : `systemctl enable --now am-stub`

INSTALLATION & UTILISATION SOUS LINUX

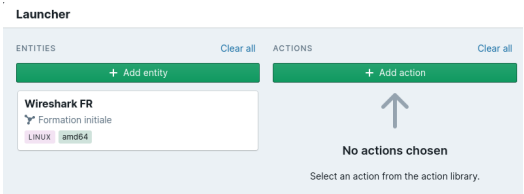
LANCEMENT D'UNE ACTION

- Dans un navigateur web, ouvrir `http://am.hns-platform.com`
- Retrouver l'entité wireshark qui nous concerne (utiliser les filtres à gauche).
- Cliquer sur « Run action on this entity »

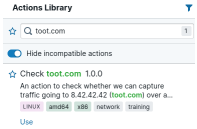


LANCEMENT D'UNE ACTION

Ajout d'une action

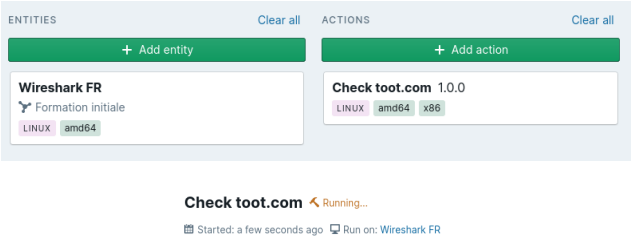


Sélection d'une action



LANCEMENT D'UNE ACTION

Lancement

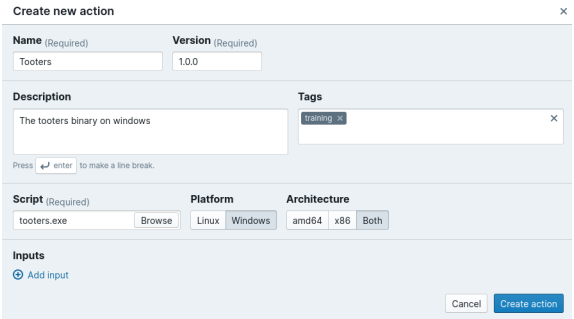


LANCEMENT D'UNE ACTION

- Stopper le service `xeyes-ng` sur la machine ubuntu
- `systemctl stop xeyes-ng`
- Vérifier que `toot.com` n'est plus ouvert dans un navigateur
- Relancer l'action 

CRÉATION D'UNE ACTION SIMPLE BINAIRE UNIQUE

- Dans l'onglet actions, cliquer sur `Create action...`
- Remplir les champs puis cliquer sur créer



INSTALLATION

2 fichiers

- `stub_windows-amd64.exe` : Le binaire qui va télécharger l'agent réel
- `config.yaml` : La configuration du stub (ne change jamais, optionnel dans le futur)

Lancer le binaire. Celui ci va automatiquement s'enregistrer en tant que service.

LANCEMENT D'UNE ACTION

Similaire au lancement d'action sous linux

- Lancer l'action juste créée sur la machine Windows
- Vérifier le fonctionnement en allant vérifier sur `toot.com` que la machine remonte bien son UUID
- On peut aussi vérifier via l'action de vérification que la valeur retournée est de nouveau `VULN`

CRÉATION D'UNE ACTION COMPLEXE

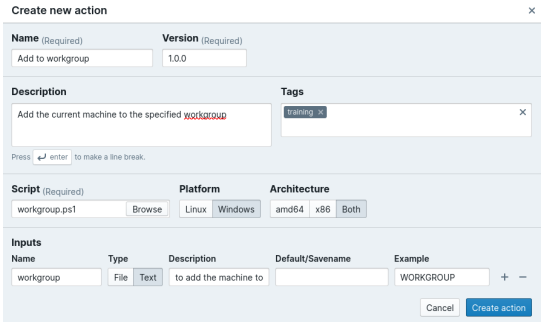
CHANGER LE WORKGROUP D'UNE MACHINE WINDOWS

Powershell !

- Les exécutables finissant par `.ps1` sont automatiquement exécutés dans un environnement powershell
- Créer un fichier `workgroup.ps1` avec le contenu suivant :
  `Add-Computer -WorkGroupName $args[0]`
- Créer une action prenant un paramètre et la lancer en précisant un nom de workgroup de votre choix

CRÉATION D'UNE ACTION COMPLEXE

CHANGER LE WORKGROUP D'UNE MACHINE WINDOWS



ALLER PLUS LOIN

API

- Enchainement séquencé d'actions
- Automatisation
- Réutilisation facile
- Documenté