Active Defense workshop- Prep guide

Histoire de ne pas passer la séance à faire des install, voici la liste des outils dont nous allons avoir besoin. Je vous recommande de les installer avant de venir, y compris ce qui est marqué 'optionnel' 😊

J'ai découpé en deux parties, nous ferons la partie 2 si le temps le permet. C'est parti :

Linux

Première partie: Envoy

Docker

Docker sera utilisé pour déployer et tester Envoy en local.

```
sudo apt install docker.io
```

[OPTIONNEL] Docker-compose

Permet de simplifier le déploiement en local. Recommandé sauf si vous aimez vous débrouiller à taper des commandes docker complexes 😊

```
sudo apt install docker-compose
```

Go

Prérequis pour utiliser tinygo.

Download https://go.dev/dl/go1.19.5.linux-amd64.tar.gz

```
rm -rf /usr/local/go && tar -C /usr/local -xzf go1.19.5.linux-amd64.tar.gz
```

```
export PATH=$PATH:/usr/local/go/bin
```

Tinygo

Nécessaire pour compiler notre plugin de défense active.

```
wget https://github.com/tinygo-org/tinygo/releases/download/v0.26.0/tinygo_0.26.0_amd64.deb
```

```
sudo dpkg -i tinygo_0.26.0_amd64.deb
```

[OPTIONNEL] Burpsuite

Pas vraiment indispensable pour le premier leurre que j'aimerais vous faire coder, mais vous sera utile pour tester d'autres types de leurres plus avancés.

Visitez https://portswigger.net/burp/releases/community/latest

Lancez l'installeur

Seconde partie: Kyma

Kubectl

Permets d'effectuer des opérations sur un cluster kubernetes. Prérequis pour installer Kyma.

```
curl -LO "https://dl.k8s.io/release/$(curl -L -s
https://dl.k8s.io/release/stable.txt)/bin/linux/amd64/kubectl"
```

Kyma

Ici deux options: soit installer Kyma en local, soit utiliser un 'trial account' dans le cloud SAP. L'install du trial account prend du temps donc prenez-vous y à l'avance :)

Installer Kyma en local:

- Vérifiez que vous avez bien installé docker
- Vérifiez que vous avez bien installé kubectl
- Installez k3d
  - `curl -s https://raw.githubusercontent.com/k3d-io/k3d/main/install.sh | bash`
- Installez Kyma CLI
  - `curl -Lo kyma.tar.gz "https://github.com/kyma-project/cli/releases/download/$(curl -s https://api.github.com/repos/kyma-project/cli/releases/latest | grep tag_name | cut -d '"' -f 4)/kyma_Linux_x86_64.tar.gz" \ && mkdir kyma-release && tar -C kyma-release -zxvf kyma.tar.gz && chmod +x kyma-release/kyma && sudo mv kyma-release/kyma /usr/local/bin \ && rm -rf kyma-release kyma.tar.gz`
- Lancez les commandes suivantes:
  - `kyma provision k3d`
  - `kyma deploy`
- Le Dashboard GUI peut être lancé avec cette commande:
  - `kyma dashboard`

Utiliser Kyma dans un trial account ('BTP Kyma'):

- Visitez https://account.hana.ondemand.com/ and créez un compte, puis faites un login.
- Cliquez 'Trial Home'
- Cliquez 'Go to your trial account'
- Cliquez 'trial'
- Cliquez 'Enable Kyma'
- Un fois l'installation terminée (prend environ 30 minutes):
  - Cliquez 'Link to dashboard'
  - Notez l'adresse de l'API Server (du style: https://api.**c-472f8b7**.kyma.ondemand.com), nous aurons besoin de la partie en gras pour déployer en remote
- Suivez les étapes décrites ici pour connecter votre kubectl à votre instance BTP: https://developers.sap.com/tutorials/cp-kyma-download-cli.html

[OPTIONNEL] Dockerhub

Pour déployer une image sur kubernetes, nous allons utiliser la registry de dockerhub. Si vous voulez utiliser mon image de démo (valvolt2/myapp:1.0) alors il n'y a rien à faire de particulier. Par contre si vous voulez (plus tard) utiliser de la défense active sur votre propre appli alors vous aurez besoin de téléverser cette appli sur dockerhub – pour ca vous aurez besoin d'un compte.

Visitez https://hub.docker.com/

You're all set!

Windows

Première partie: Envoy

Docker

Docker sera utilisé pour déployer et tester Envoy en local.

Sur Windows, le plus simple est d'installer Docker Desktop (dispo ici: https://docs.docker.com/desktop/install/windows-install/). C'est un logiciel gratuit pour les entreprises de moins de 250 personnes ou si pour usage non-commercial.

[OPTIONNEL] Docker-compose

Permet de simplifier le déploiement en local. Recommandé sauf si vous aimez vous débrouiller à taper des commandes docker complexes 😊

Rien de spécial à faire si vous avez docker desktop, docker-compose est installé automatiquement.

Go

Prérequis pour utiliser tinygo.

Téléchargez et installez https://go.dev/dl/go1.19.5.windows-amd64.msi

Tinygo

Nécessaire pour compiler notre plugin de défense active.

Download https://github.com/tinygo-org/tinygo/releases/download/v0.26.0/tinygo0.26.0.windows-amd64.zip

Decompressez le fichier

Déplacez le répertoire là ou vous voulez (par exemple: C:\)

Mettez votre PATH à jour, par exemple:

```
set PATH=%PATH%;"C:\tinygo\bin"
```

[OPTIONNEL] Burpsuite

Pas vraiment indispensable pour le premier leurre que j'aimerais vous faire coder, mais vous sera utile pour tester d'autres types de leurres plus avancés.

Visitez https://portswigger.net/burp/releases/community/latest

Lancez l'installeur

Seconde partie: Kyma

Chocolatey

Chocolatey simplifie l'installation de kubectl et de k3d. Je vous recommande de l'installer. Si non, vous allez devoir trouver un autre moyen d'installer les autres outils de la liste.

Ouvrez un prompt PowerShell en Admininstrator, puis executez:

```
Set-ExecutionPolicy Bypass -Scope Process -Force;
[System.Net.ServicePointManager]::SecurityProtocol =
[System.Net.ServicePointManager]::SecurityProtocol -bor 3072; iex
((New-Object
System.Net.WebClient).DownloadString('https://chocolatey.org/install.p
s1'))
```

Kubectl

Permets d'effectuer des opérations sur un cluster kubernetes. Prérequis pour installer Kyma.

Sous PowerShell, lancez:

```
choco install kubernetes-cli
```

Kyma

Ici deux options: soit installer Kyma en local, soit utiliser un 'trial account' dans le cloud SAP. L'install du trial account prend du temps donc prenez-vous y à l'avance :)

Installer Kyma en local:

- Vérifiez que vous avez bien installé docker

- Vérifiez que vous avez bien installé kubectl
- Installez k3d
    - `choco install k3d -y`
- Installez Kyma CLI
    - `choco install kyma-cli`
- Lancez les commandes suivantes:
    - `kyma provision k3d`
    - `kyma deploy`
- Le Dashboard GUI peut être lancé avec cette commande:
    - `kyma dashboard`

Utiliser Kyma dans un trial account ('BTP Kyma'):

- Visitez https://account.hana.ondemand.com/ and créez un compte, puis faites un login.
- Cliquez 'Trial Home'
- Cliquez 'Go to your trial account'
- Cliquez 'trial'
- Cliquez 'Enable Kyma'
- Un fois l'installation terminée (prend environ 30 minutes):
    - Cliquez 'Link to dashboard'
    - Notez l'adresse de l'API Server (du style: https://api.**c-472f8b7**.kyma.ondemand.com), nous aurons besoin de la partie en gras pour déployer en remote
- Suivez les étapes décrites ici pour connecter votre kubectl à votre instance BTP: https://developers.sap.com/tutorials/cp-kyma-download-cli.html

[OPTIONNEL] Dockerhub

Pour déployer une image sur kubernetes, nous allons utiliser la registry de dockerhub. Si vous voulez utiliser mon image de démo (valvolt2/myapp:1.0) alors il n'y a rien à faire de particulier. Par contre si vous voulez (plus tard) utiliser de la défense active sur votre propre appli alors vous aurez besoin de téléverser cette appli sur dockerhub – pour ca vous aurez besoin d'un compte.

Visitez https://hub.docker.com/

You're all set!