Documentation d'Installation Complète - Projet Proxmox avec Kali Linux, Metasploitable et Suricata

1. Pré-requis

Avant de commencer l'installation, s'assurer que nos serveur ou machine virtuelle sur Proxmox répond aux conditions suivantes :

- **Proxmox VE** installé et configuré.
- Connexion à Internet pour télécharger les images ISO nécessaires.
- Les ressources système suivantes sont recommandées :
    - **CPU** : 2 Cores minimum.
    - **RAM** : 8 Go (ou plus).
    - **Disque** : 50 Go minimum pour la virtualisation.

2. Téléchargement des ISO nécessaires

Télécharger les images suivantes pour les installer sur les machines virtuelles :

- **Kali Linux** : Téléchargement Kali Linux.
- **Metasploitable** : Téléchargement Metasploitable 2.
- **Ubuntu Server** pour installer Suricata : Téléchargement Ubuntu Server.

Stockage des ISO sur Proxmox

1. Connecte à l'interface web de Proxmox via https://<IP_du_serveur>:8006.
2. Dans l'onglet **"Datacenter"**, sélectionner **Storage** (par défaut, c'est souvent "local").
3. Aller dans l'onglet **ISO Images** et télécharger les fichiers ISO de Kali, Metasploitable, et Ubuntu.

3. Création des Machines Virtuelles

3.1 Création de la VM pour Kali Linux

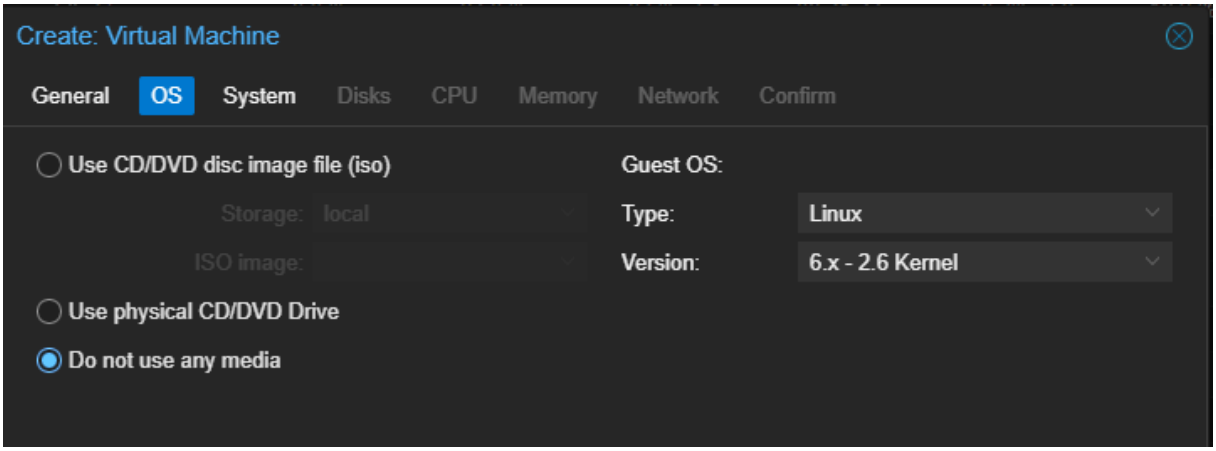
1. Dans l'interface web de Proxmox, cliquer sur **Create VM**.
2. Remplis les informations suivantes :
    - **Nom de la VM** : Kali_Linux.
    - **OS Type** : Linux, Debian 10/11 (selon la version de Kali).
    - **ISO Image** : Sélectionner l'ISO de Kali Linux que on a téléchargé.

- **RAM** : 2 Go minimum.
- **CPU** : 2 cœurs.
- **Disque** : 20 Go minimum (en utilisant un disque virtuel).

3. Une fois la VM créée, démarre-la et suis le processus d'installation de Kali Linux, en configurant l'interface réseau pour qu'elle soit sur le même sous-réseau que Metasploitable.

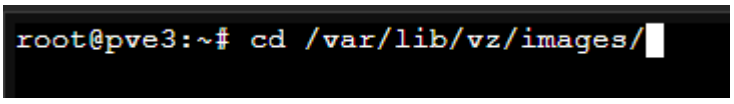
3.2 Création de la VM pour Metasploitable

1. Clique sur **Create VM** dans Proxmox.
2. Remplis les informations suivantes :

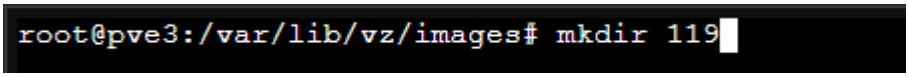


   - **Nom de la VM** : Metasploitable.
   - **OS Type** : Linux, Other Linux (32-bit).
   - **RAM** : 8 Go.
   - **CPU** : 2 cœur.
   - **Disque** : 32 Go.

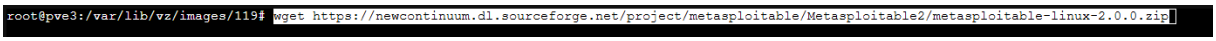
3. Ce rendre dans le shell du node proxmox



4. Créer un dossier avec le même id que la vm crée



5. Télécharger le fichier metasploitable et le mettre dans le fichier créer



6. Unzip le fichier

```
root@pve3:/var/lib/vz/images/119# unzip metasploitable-linux-2.0.0.zip
```

7. Ce rendre dans le fichier puis rendre le fichier lisible par proxmox

```
root@pve3:/var/lib/vz/images/119/Metasploitable2-Linux# qemu-img convert -f vmdk Metasploitable.vmdk -O qcow2 Metasploitable.qcow2
```

8. Déplacer le fichier a la racine

```
root@pve3:/var/lib/vz/images/119/Metasploitable2-Linux# Mv Metasploitable.qcow2 ../
```

9. Editer la configuration de la VM 119 pour lui dire d'utiliser le fichier pour boot

```
root@pve3:/var/lib/vz/images/119# nano /etc/pve/qemu-server/119
```

10. Modifier la ligne ide0 :

```
  GNU nano 7.2
boot: order=ide0;ide2;net0
cores: 2
cpu: x86-64-v2-AES
ide0: file=local:119/Metasploitable.qcow2,size=32G
ide2: none,media=cdrom
memory: 8192
meta: creation-qemu=9.0.2,ctime=1742922276
name: projet2metasploitable
net0: virtio=BC:24:11:7F:62:9C,bridge=vmbr0,firewall=1
numa: 0
ostype: l26
scsihw: virtio-scsi-single
smbios1: uuid=d0cca221-d597-4f1e-92f5-d44303a07b9a
sockets: 1
vmgenid: b67dd470-4dea-4bf4-b36c-50cdf77d573e
```

11. Attache l'image disque Metasploitable à la VM, puis démarre-la. Metasploitable est une machine prête à l'emploi, donc une fois lancée, tu peux commencer à l'exploiter immédiatement.

```
msfadmin@metasploitable:~$
```

3.3 Création de la VM pour Suricata

1. Clique sur **Create VM**.
2. Remplis les informations suivantes :
   - **Nom de la VM** : Suricata.
   - **OS Type** : Linux, Ubuntu 20.04.
   - **ISO Image** : Sélectionne l'ISO Ubuntu Server.
   - **RAM** : 2 Go.

- **CPU** : 2 cœurs.
- **Disque** : 10 Go.

3. Démarre la VM et installe Ubuntu Server normalement. Une fois le système installé, il est temps de configurer Suricata.

4. Installation et Configuration de Suricata sur Ubuntu

1. Connecte-toi à la VM Ubuntu et mets à jour le système :

sudo apt update && sudo apt upgrade -y

```
suricata@suricata:~$ sudo apt update && sudo apt upgrade -y
```

2. Installe Suricata :

sudo apt install suricata -y

```
suricata@suricata:~$ sudo apt install suricata -y
```

3. Configure Suricata pour surveiller le réseau. Ouvre le fichier de configuration de Suricata :

sudo nano /etc/suricata/suricata.yaml

- Cherche l'option interface: eth0 et assure-toi que l'interface réseau correspond à celle utilisée par ta machine.

```
# Linux high speed capture support
af-packet:
  - interface: net0
```

4. Démarre Suricata :

sudo systemctl enable suricata

```
suricata@suricata:~$ sudo systemctl enable suricata
Synchronizing state of suricata.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable suricata
```

sudo systemctl start suricata

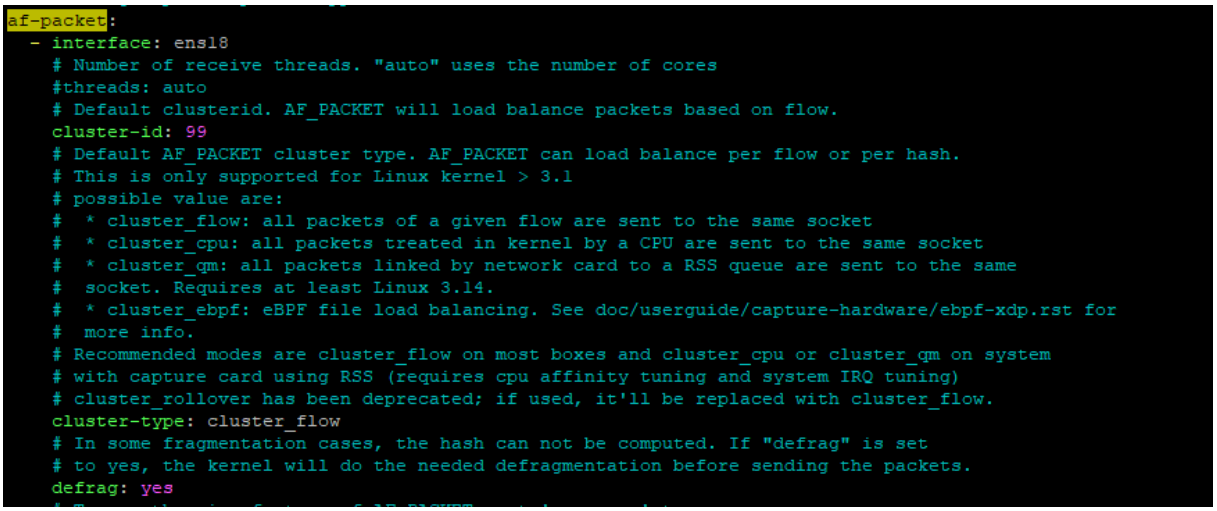
```
suricata@suricata:~$ sudo systemctl start suricata
```

5. Mettre suricata en mode écoute :

ip a puis récupérer l'interface réseau, en l'occurrence ens18

```
suricata@suricata:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
```

nano /etc/suricata/suricata.yaml puis mettre la bonne carte reseau



6.

5. Recuperation des logs suricata

Installation de Frontail

sudo npm install -g frontail

Recuperation des logs en direct :

frontail /var/log/suricata/eve.json

5. Configuration Réseau dans Proxmox

Il est important que les machines Kali, Metasploitable et Suricata soient dans le même sous-réseau pour qu'elles puissent communiquer et que Suricata puisse détecter les attaques.

1. Assurer que toutes les VM sont dans un réseau virtuel isolé ou dans le même réseau physique (via mode Bridge ou NAT).
2. Configure les adresses IP sur chaque VM (**6. Tests d'Attaque**

6.1 Scan avec Nmap

Depuis la VM Kali, faire un scan de Metasploitable :

nmap -A 192.168.1.77

Suricata doit détecter ce scan et générer des alertes dans les logs.

6.2 Exploitation de Vulnérabilités avec Metasploit

1. Lancer **Metasploit** sur Kali :

msfconsole

2. Sélectionne un exploit pour Metasploitable, par exemple, une vulnérabilité FTP :

use exploit/unix/ftp/vsftpd_234_backdoor

set RHOST 192.168.1.77

exploit

3. Vérifie les logs de Suricata pour l'alerte générée par cette exploitation.

7. Sécurisation avec Suricata

1. Suricata offre la possibilité de créer des règles personnalisées pour bloquer certaines attaques. Par exemple, pour détecter et bloquer des tentatives de brute force FTP, crée une règle spécifique dans le fichier /etc/suricata/rules/:

alert ftp any any -> any any (msg:"Brute Force FTP"; content:"USER";)

2. Redémarre Suricata pour appliquer la règle :

sudo systemctl restart suricata

8. Analyse des Logs et Rapport

Suricata stocke les alertes dans /var/log/suricata/. On peut analyser ces logs pour comprendre quelles attaques ont été détectées.

cat /var/log/suricata/eve.json

On y trouvera des informations sur les attaques détectées par Suricata.