Document d’exploitation

à usage interne

Sommaire :

1. Mise en service

- Installation
    - Pfsense :
    - Ubuntu LTS :
    - Git
    - VirtualBox :
    - PentBox
    - Screen :
    - Document d'exploitation de l'infrastructure réseau

2. Supervision

- Supervision système
    - 1.1. Hôte (Windows 10)
    - 1.2. Miller (Ubuntu Desktop) & Gargantua
        1. Murphy (pfsense)
        2. Supervision applicative de Gargantua (PentBox)
    - Création et exécution de scripts de supervision
    - Configuration et gestion de PentBox pour le honeypot

3. Sauvegardes

- Stratégie appliquée
- Sauvegardes hebdomadaires
- Existe-t-il des sauvegardes plus spécifiques par rapport aux services ?

4. Restauration

- Restauration du système et du côté applicatif

5. Procédure d’arrêt

- Pour arrêter les différentes machines

6. Support

- Contact et horaires de support

- ## Installation

pas besoin de détailler un plan d'installation puisqu'il en existe pleins sur internet, voici les tutoriels qui ont été utilisés pour la mise en place de ce projet :

Pfsense : https://www.it-connect.fr/installation-de-pfsense%EF%BB%BF/
Ubuntu-lts : https://ubuntu.com/tutorials/install-ubuntu-desktop#1-overview
Git : sudo apt install git (à entrer dans un invité de commande linux (ubuntu))
VirtualBox : *https://www.virtualbox.org/*
PentBox (honeypot) : https://youtu.be/f5Xqy3ur1sw?si=SQ7aVy7X2pIZFBL9&t=194
Screen : (Permet de faire tourner un terminal en permanence) sudo apt-get install screen (à entrer dans un invité de commande linux (gargantua))

• Document d'exploitation l'infrastructure réseau

Nous allons détailler la supervision des différents systèmes par machine.

- ## Supervision

- ## Supervision système

1.1. Hôte (Windows 10)

- **Supervision Système** :
  - **Processus** : Utilisation du gestionnaire des tâches
  - **Espace Disques** : Utilisation de l'explorateur de fichiers ou **de l'outil d'administration de disque Windows 10** : Ouvrez la barre de recherche windows et écrivez : Créez et partitionner des disques.

    ou alors : Paramètre de stockage

  - **Utilisation CPU et Mémoire** : Utilisation du gestionnaire des tâches.
  - **Gestion des périphériques :** taper Gestion des périphériques

1.2. Miller (Ubuntu Desktop) & Gargantua

- **Supervision Système** :
  - **Processus** : Utilisation de ps, top, ou htop pour vérifier les processus.
  - **Espace Disques** : Utilisation de df -h.
  - **Utilisation CPU et Mémoire** : Utilisation de top ou htop sur les machines linux
- **Supervision Disque**:
  - **Processus** : Utilisation de ps, top, ou htop pour vérifier les processus.
  - **Espace Disques** : Utilisation de df -h.
  - **Utilisation CPU et Mémoire** : paramètres disques dur de ubuntu desktop

Supervision Applicative de Gargantua (PentBox):

Utilisation de Screen :

1. Créer un Script de Supervision

https://doc.ubuntu-fr.org/screen

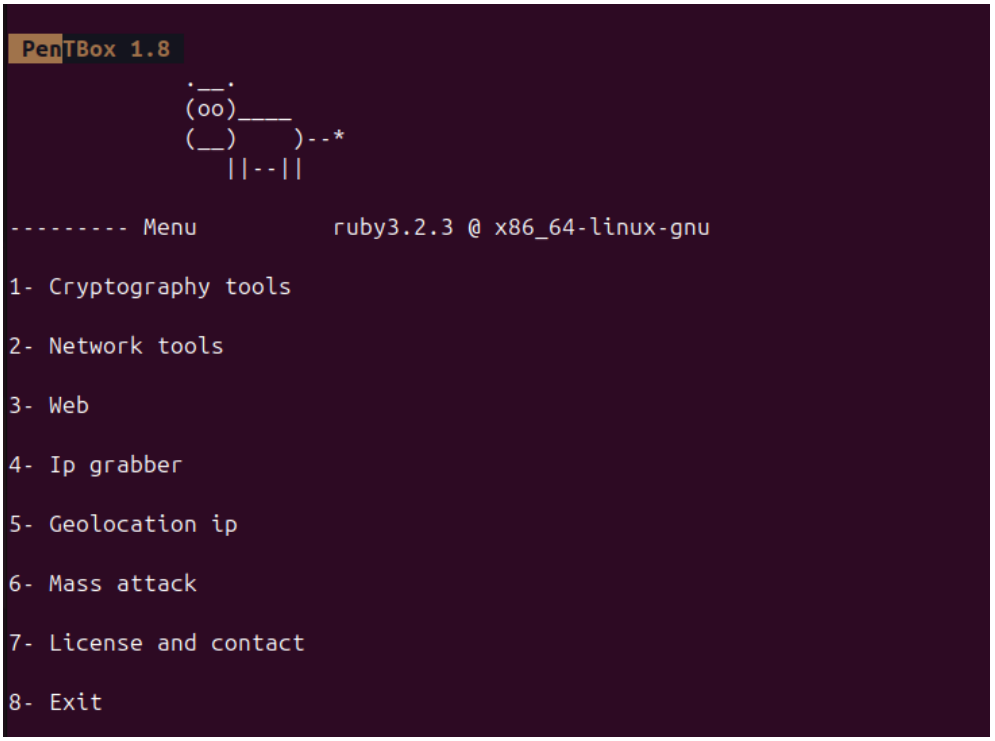
(vous fournira toutes la documentation de comment faire tourner ou arrêter le screen qui contient PentBox)

2. PentBox :

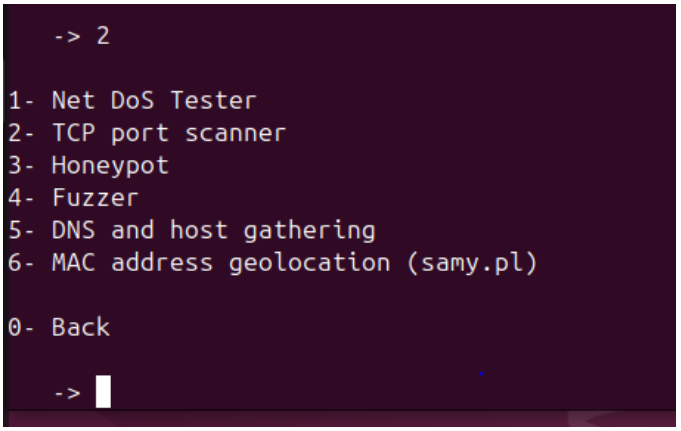
après avoir installer PentBox, allez dans le répertoire PentBox et lancer la commande : ./pentbox.sh

1. **Comment modifier le HoneyPot**

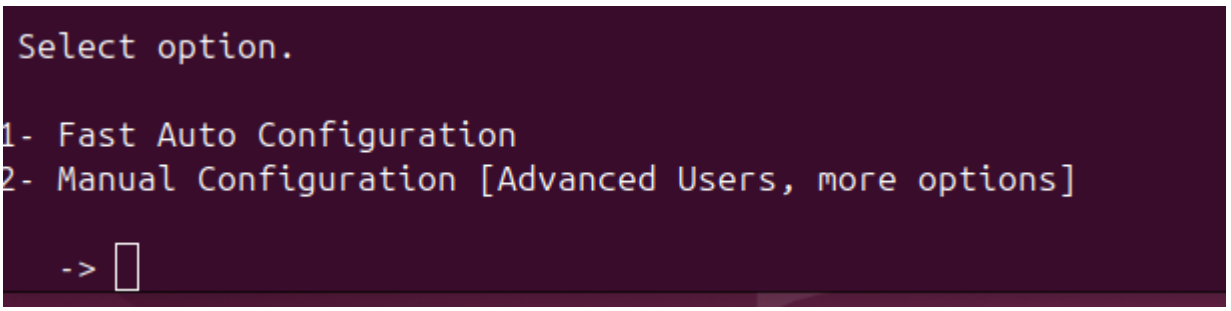
   Choisissez le Chiffre 2 qui correspond à Network Tools :



2. **Puis entrez 3 pour accéder au services honeypot**



3. **Puis choisissez 1 ou 2**



1. **si vous choisissez 1 :**

Dans le cadre du projet c'est ce que j'ai utilisés, il s'agit d'une page internet accessible sur : votre-ip:80, il n'y a donc rien d'autre à faire, pour lancer le processus

Pour arrêter le processus, éteindre le terminal Screen, ou alors faire un ctrl-c

2. **si vous choisissez l'option 2** :

- Voici les différentes étapes :
  - **Choisir le port voulu** : 80
  - **chemin du Document Root** : : *Spécifiez le chemin du répertoire où se trouvent les fichiers HTML, ici le fichier html qui est utilisé pour afficher le site internet. une page de connexion à un service interne : :* /home/desktop/nepting-payments-internals/index.html
  - **Activer ou désactiver l'alerte Sonor**e : yes ou no
  - **Fichier log** :
    - pathLog : /home/desktop/nepting-payments-internals/logs/log_honeypot.txt

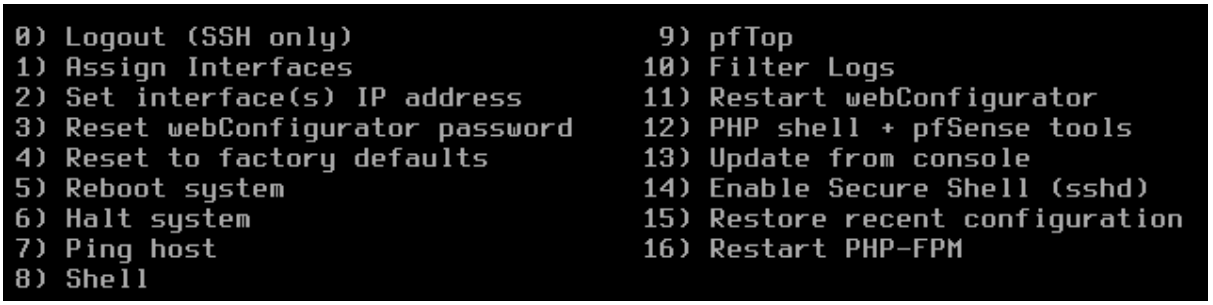
1. Murphy (pfsense)

Supervision Système :

- **Processus :** Utilisez l'interface de Pfsense pour vérifier l'état des processus. ou la console. si vous souhaitez modifier les paramètres de la machine, modifier les paramètres de la VM dans virtualBox
- **CPU & Mémoire :** Consultez Diagnostics > System Activity > CPU usage pour l'utilisation de la mémoire
- **DISQUE :** Diagnostics > System Activity > Disk usage
- pour modifier la taille du disque, allez modifier directement dans les paramètres de la vm pour virtualBox

Supervision Applicative :

pour modifier les interfaces ou les ip, l'interface parle d'elle même



entrez les chiffres suivants dans l'interface pfsense

1. **pour modifier les interfaces :** (associé les cartes réseaux au interfaces de pfsense)

2. **pour modifier les ip** : configurer les dhcp des interfaces pfsenses

- ## Sauvegardes

- ### Stratégie appliquée

Sauvegarde hebdomadaire.

Ces scripts permettent de créer des sauvegardes complètes hebdomadaires des données critiques pour chaque machine. Les **paramètres** spécifient le répertoire de **destination** pour les **sauvegardes** et les **répertoires** ou **fichiers** à inclure dans la sauvegarde.

- ### Sauvegardes hebdomadaires

un fichier de backup est créé, il agit comme une tache cron, ce script doit être exécutée tout les jours, avec la commande :

1. **Gargantua (honeypot)**

Comment lancer la sauvegarde ?

la commande lancée une fois par semaine. 0 2 * * 0 /usr/local/bin/backup_full_gargantua.sh

Où se trouve le fichier de sauvegarde ?
le fichier est disponible dans ce répertoire: `/usr/local/bin/backup_full_gargantua.sh` :

Comment modifier le fichier de sauvegarde ?
Pour le modifier utiliser : nano `/usr/local/bin/backup_full_gargantua.sh` :

2. Miller (serveur web)

Comment lancer la sauvegarde ?
la commande à lancer une fois par semaine est : `0 3 * * 0 /usr/local/bin/backup_full_miller.sh`

Où se trouve le fichier de sauvegarde ?
le fichier est disponible dans ce répertoire
`/usr/local/bin/backup_full_miller.sh`

Comment modifier le fichier de sauvegarde ?
Pour le modifier utiliser : nano `/usr/local/bin/backup_full_miller.sh` :

Existe t'il des sauvegardes plus spécifiques par rapport au services ?

Non, c'est sauvegardes font une backup entières des machines, il est aussi possible de faires des **backups** des **vm via virtual box**, **en créant des snapshots**

Voici une ressource pour réaliser l'opération :
https://www.it-connect.fr/la-gestion-des-snapshots-avec-virtualbox%EF%BB%BF/

A quoi servent les sauvegardes ?

Concrètement, ses fichiers nous servent à faire des backup, des fichiers de configurations spécifiques à chaque système.

Pour Gargantua il sauvegarde :

1. les fichiers de configurations spécifique à la machine
2. les paramètres réseaux (quel ip lui est associé)
3. log d'activité du honey pot.
4. configuration du honeypot

Pour Miller il sauvegarde :

1 les fichiers de configuration spécifique à la machine
2. les paramètres réseaux
3. en backup des fichiers spécifique liés au client et au service interne de l'entreprise (portail entreprise)

- ## Restauration

- **Restauration du système et du coté applicatif**

Suivre le module installation pour restaurer les différentes machines

Chaque machine contient une ressource de comment l'installer (voir module installation page 8)

chaque logiciel est aussi accompagné dans ce document d'une ressource de comment l'installer

- ## Procédure d'arrêt

Pour arrêter les différentes machines :

Hôte (windows 10)**:**

éteindre l'ordinateur en s'assurant que les machines virtuelles sont bien à l'arrêt

Gargantua, miller (ubuntu lts**) :**

stopper la machine via virtualbox, en prenant soins de fermer les applications sur les vm, en cliquant sur : **Enregistrer l'état de la machine**

- ## Support

Pour toute question techniques, vous pouvez contacter le service IT

En semaine : contacter le service it

service it : nils.jaudon@siwhite.com

disponible : de 8h à 17h le lundi, mardi, mercredi, jeudi, vendredi,

Pour le weekend : contacter les personnes d'astreintes

personne d'astreinte : jeanluc.jordin@siwhite.com

disponible : 24h/24 du **vendredi** à **17h** jusqu'au **lundi** à **8h**.