INFRA SI

HoneyPot

PentBox / honeypot

Mise en service

référence	*nils_jaudon_projet_infra_si.docx*
version	1.1
statut	
créé le	*13/06/2024 15:29:00*
par	Nils JAUDON
mis à jour le	*09/06/2024 17:21:00*
par	Nils JAUDON
validé le	*03/06/2024 17:21:00*
par	
diffusé le	16/06/2024
à	Jullien LALLEMAND
Péremption, archivage et restriction de diffusion *Nature de la restriction : confidentiel, diffusion restreinte, diffusion interne, restriction annulée*	Usage interne

Table des matières

• Document d'architecture technique Projet Infra

• Fonctionnalité et domaine applicatif

Cocher la case correspondante

Domaine Data Management/aide à la décision	
Domaine Investigation clinique	
Domaine Informatique scientifique	
Domaine Support aux départements	
Domaine Outils collaboratifs et audiovisuels	
Secteur Infrastructure logicielle	X
Secteur Infrastructure réseau	X
Secteur Ingénierie poste de travail	

• Architecture matérielle

1. PC WINDOWS 10 (PHYSIQUE) (hôte)
1. VM VIRTUALBOX UBUNTU-LTS (virtuelle) (serveur)
1. VM VIRTUALBOX PFSENSE (Virtuelle) (pare feu)
1. VM VIRTUALBOX UBUNTU-LTS (virtuelle) (honeypot)

• Architecture logicielle

1. PC Windows 10
   - **Système d'exploitation :** Windows 10
   - **Rôle :** Utiliser l'administration et l'accès aux machines virtuelles.
   - **Logiciels :** Bureautique & VirtualBox.

Lien pour télécharger virtual box : https://www.virtualbox.org/

2. VM Virtual Box Ubuntu LTS (Miller)

- **Système d'exploitation :** Ubuntu-LTS (64 bit)
- **Rôle :** Machine interne principal de l'entreprise qui contient des informations confidentielles (base de données, site interne à l'entreprise, outil de gestion d'administration services de fichiers).
- **Logiciels :**
    - Apache2 (serveur web)
    - Visual Studio Code : (Développement)
    - DataGrip : (Gestion de base de donnée)

3. VM Virtualbox Ubuntu LTS (Gargantua)

- **Système d'exploitation :** Ubuntu-LTS (64 bit)
- **Rôle :** Gargantua est une référence à interstellar, il agit comme un trou noir, configuré pour simuler des services et des vulnérabilités afin **d'attirer** les attaquants dedans. Il est conçu pour détecter et analyser les tentatives d'intrusions sans compromettre la sécurité du réseau interne. **ici il agira en tant que site web interne à l'entreprise (Portails d'Entreprise)**
- **Logiciels :**
    - Python3.12 (Gestion des librairies + Langage de programmation)
    - PentBox (Outil pour configurer / crée un honeypot
    - Git (Permet d'installer PentBox)
    - Screen (Gestions des terminaux)

4. VM VirtualBox PFSENSE (Murphy)

- **Système d'exploitation :** Pfsense freebsd (64 bit)
- **Rôle :** Murphy est un pare feu, il sert à analyser le trafic réseau entrant et sortant, il sert à segmenter notre réseaux avec nos différentes interfaces réseaux, La mise en place d'un DHCP, Réseau Interne LAN / DMZ, Vlan
- **Logiciels :** Aucun à part l'installation de pfsense

- ## Architecture réseau et sécurité

Description de l'architecture réseau, les flux associés les règles de sécurité du pare-feu, ainsi que le rôle (ici le rôle des interface pfsense)

Nom de la machine	Interface Pfsense	Adresse IP	VLAN	Fonctionnalité	Role
Hôte (windows 10)	Ethernet	192.168.1.34	N/A	Ethernet	hôte
Miller (Ubuntu Desktop)	em1 (lan) 192.168.56.1/24	192.168.56.10	100	DHCP lan : 192.168.56.10 192.168.56.50	permet dhcp sur le réseau interne lan
Gargantua (honeypot)	em2 (DMZ) 192.168.100.1/24	192.168.100.10	150	DHCP dmz 192.168.100.10 192.168.100.50	permet dhcp sur le réseau interne dmz
Murphy (pfsense)	em0(wan) 192.168.1.16/24	192.168.1.16	N/A	filtrage/configuration interface	Pare Feu

DMZ :

- Limiter strictement le trafic sortant de la DMZ vers Internet.

LAN

- Autoriser le trafic interne entre Miller et Gargantua pour services internes.
- Bloquer le trafic sortant non autorisé vers Internet depuis le LAN.

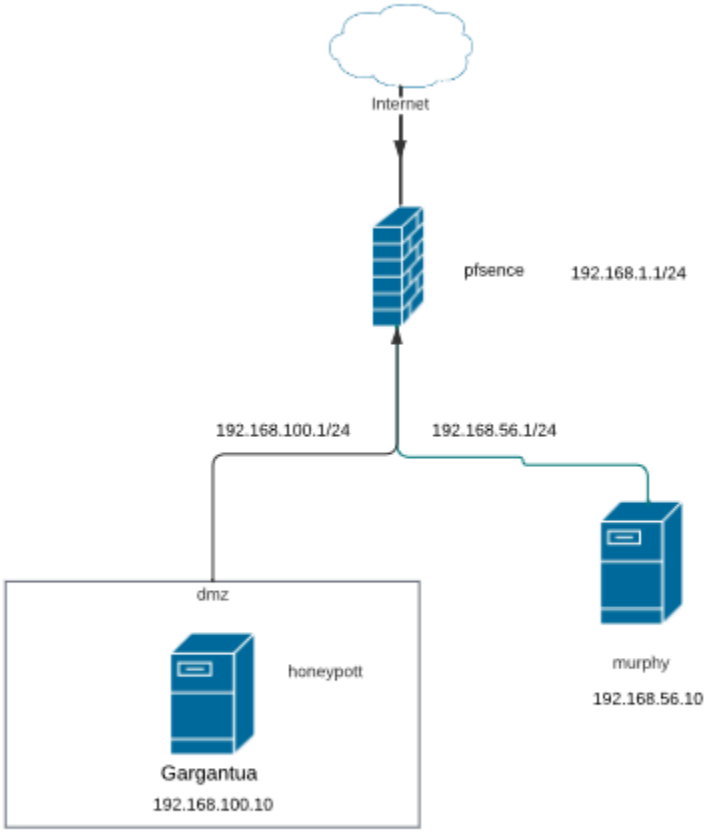
WAN

- Bloquer le trafic entrant non sollicité de l'Internet vers le LAN.
- Autoriser le trafic sortant nécessaire vers Internet depuis le LAN.

VLAN

- **Dans un futur il sera surement amené à avoir plusieurs services au seins d'un réseau interne, c'est pour cela que les vlans.**
- **pourquoi vlan 99? car le vlan 99 est en bonne pratique associé au PC Administration, et 150 est associé au vlan DMZ**

Schéma :



Pourquoi avoir mis une dmz dans un réseau interne ?

1. Isolation des Services Exposés
2. Sécurité Renforcée
3. Analyse des Menaces
4. Meilleure Gestion des Ressources

Ici mes clients sont uniquement sur le schéma, et ne sont pas mis en place due à un manque de ressources de mon hôte windows 10, mais dans la réalité, il le serait.

- ## 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

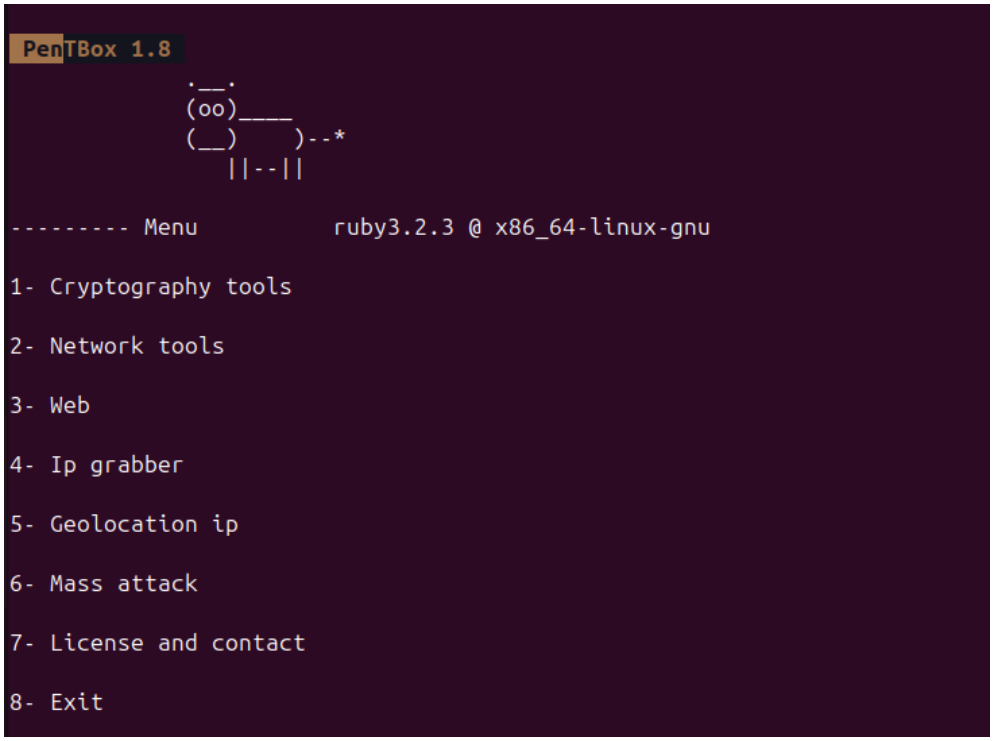
(vous fournira toutes la documentation de comment faire tourner ou arrêter le screen qui contient PentBox)

2. PentBox :

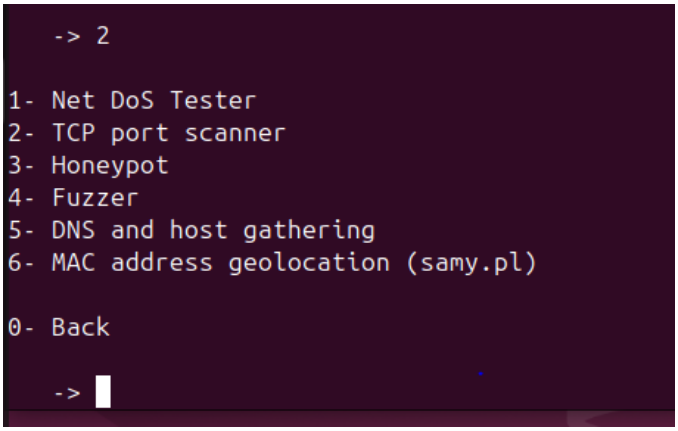
après avoir installer PentBox, allez dans le répertoire PentBox et lancer la commande : ./pentbox.sh

1. **Comment modifier le HoneyPot**

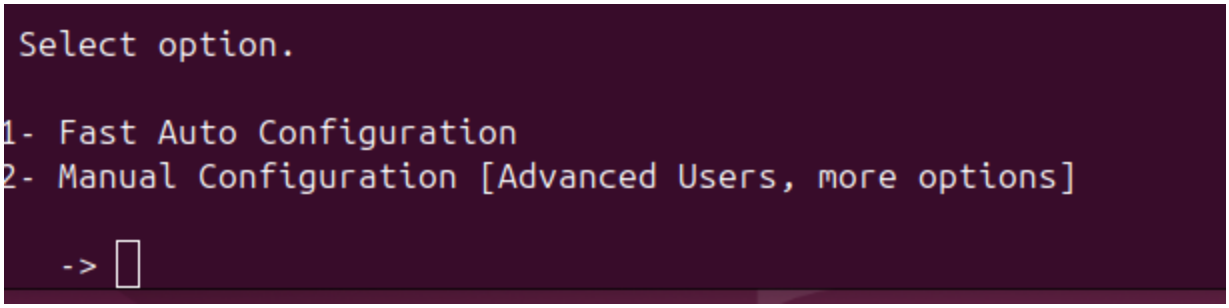
   Choisissez le Chiffre 2 qui correspond à Network Tools :



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

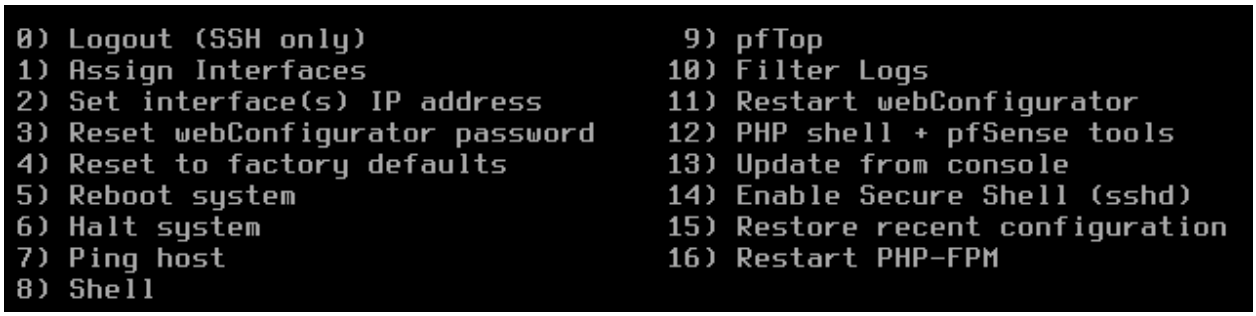
1. Murphy (pfsense)

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**.