Documentation du Mini-Projet : Mise en place d'un Honeypot avec Cowrie

Objectif du projet

Mettre en place un honeypot de type SSH avec l'outil Cowrie, dans une machine virtuelle Debian, afin de :

- Simuler un serveur SSH vulnérable.

- Capturer les tentatives de connexion malveillantes.

- Enregistrer toutes les actions effectuées par l'attaquant dans un environnement piégé.

Prérequis

- VMware Workstation (ou autre hyperviseur)

- Image Debian 11 ou 12 (installée et configurée)

- Accès à un terminal root dans la VM

- Connexion Internet dans la VM

- Accès à un terminal Windows avec Nmap installé

Partie 1 : Installation de Cowrie

1. Mettre à jour les paquets :

sudo apt update && sudo apt upgrade

2. Installer les dépendances :

sudo apt install git python3-virtualenv libssl-dev libffi-dev build-essential python3-minimal python3-pip libpython3-dev python3-venv -y

3. Cloner Cowrie :

git clone https://github.com/cowrie/cowrie.git

cd cowrie

4. Configurer l'environnement virtuel :

python3 -m venv cowrie-env

source cowrie-env/bin/activate

5. Installer les dépendances Python :

pip install --upgrade pip

pip install --upgrade -r requirements.txt

6. Créer les répertoires de logs :

mkdir -p var/log/cowrie

chmod -R 700 var

7. Démarrer Cowrie :

bin/cowrie start

8. Vérifier que Cowrie tourne :

bin/cowrie status

Partie 2 : Scanner avec Nmap depuis Windows

1. Installer Nmap avec Chocolatey (si besoin) :

choco install nmap -y

2. Trouver l'adresse IP de la VM Debian :

ip a # depuis la VM

Exemple obtenu : 192.168.200.132

3. Scanner les ports depuis Windows :

nmap -p 22,2222 192.168.200.132

4. Interprétation :

- Le port 22 est fermé (car le vrai SSH est désactivé)

- Le port 2222 est ouvert : Cowrie simule un serveur SSH ici

Partie 3 : Connexion simulée à Cowrie

Depuis Windows :

ssh root@192.168.200.132 -p 2222

- Cowrie affiche un faux terminal Debian.

- Toutes les commandes sont enregistrées, mais rien n'est exécuté pour de vrai.

Partie 4 : Observation des logs

Dans la VM :

tail -f var/log/cowrie/cowrie.log

On peut y voir :

- Les tentatives de connexion

- Les mots de passe testés

- Les commandes entrées par l'utilisateur

Conclusion

Ce mini-projet a permis de comprendre le fonctionnement d'un honeypot :

- Simulation réaliste d'un terminal SSH

- Capture d'activité malveillante

- Utilisation de Cowrie dans un environnement virtuel