	TP :

Objectif : découvrir le concept d'honeypot et le mettre en place en se mettant du point de vue attaquant et attaqué.

I. Pour découvrir le principe d'un honeypot, mettons-nous en condition ;

Oublions Kali un instant et prenez une VM Ubuntu. On l'a vu que Kali était un peu une forteresse, ce serait un poil plus compliqué de mettre en place un dispositif de ce genre. Testé sur version 16 mais franchement ça ne devrait pas trop poser de problème (espérons).

Mettez-vous en LAN. Pas de WAN tant que la machine n'est pas isolée !

- Faites un petit schéma au format que vous voulez (Visio, PT, Paint…) et mettez-vous en binôme.

II. Continuons notre expérimentation ;

- Lisez la documentation de David French. La documentation est volontairement en anglais pour renforcer votre vocabulaire technique. Dès que c'est en place faites un résumé en français dans votre rapport puis tentez de tomber dans le honeypot de votre voisin.
- Le piège a-t-il fonctionné ?
- Comment le savez-vous ?

  Je peux voir les attaques réalisées dans le fichier log de cowrie
- Comment le pirate pourrait savoir qu'il est tombé dans un piège ?

III. Essayons autre chose ;

- Isolez votre machine Ubuntu « honeypottée »* du réseau et passez là en WAN.
- Que se passe-t-il sur votre honeypot ? Si cela fonctionne « trop bien », éteignez votre machine.
- Si cela ne fonctionne « pas trop », trouvez une explication rationnelle à tout cela.

IV. Tirez des conclusions sur ce que vous venez de découvrir, et documentez-vous s'il existe des alternatives à l'application testée aujourd'hui.

Le honeypots comme sont nom l'indique est un pot de miel qui vise à attirer les attaquants dans une zone contrôlée

V. Documentez ce TP et rendez-le sur Moodle dans les délais indiqués. Le barème reposera sur la qualité de votre rendu, orthographe, rédaction, explications, illustration…

Créer un honeypot sur Ubuntu 22.04.3 implique de configurer un environnement sécurisé qui attire les attaquants, pour surveiller leurs actions et analyser les attaques. Voici un guide détaillé pour créer un honeypot en utilisant l'outil **Cowrie**, un honeypot SSH/Telnet populaire, sur Ubuntu 22.04.3.

Étapes pour installer et configurer Cowrie comme honeypot :

1. Mise à jour du système

Avant de commencer, assurez-vous que votre système Ubuntu est à jour.

```
bash
Copier le code
sudo apt update && sudo apt upgrade -y
```

2. Installation des dépendances nécessaires

Cowrie a besoin de certaines dépendances pour fonctionner correctement. Installez-les avec cette commande :

```
bash
Copier le code
sudo apt install git python3 python3-virtualenv python3-dev libssl-dev
libffi-dev build-essential -y
```

3. Création d'un utilisateur dédié pour Cowrie

Pour des raisons de sécurité, créez un utilisateur dédié qui ne dispose pas de privilèges administratifs.

```
bash
Copier le code
sudo adduser --disabled-password --gecos "" cowrie
```

4. Télécharger Cowrie depuis GitHub

Connectez-vous avec l'utilisateur **cowrie** et clonez le dépôt officiel de Cowrie.

```
bash
Copier le code
sudo su - cowrie
git clone https://github.com/cowrie/cowrie
cd cowrie
```

5. Configurer un environnement virtuel Python

Créez un environnement virtuel Python pour isoler les dépendances de Cowrie.

```
bash
Copier le code
python3 -m venv cowrie-env
source cowrie-env/bin/activate
```

6. Installer les dépendances Python

Installez les dépendances Python requises pour Cowrie à l'intérieur de l'environnement virtuel.

```
bash
Copier le code
pip install --upgrade pip
pip install -r requirements.txt
```

7. Configurer Cowrie

Copiez le fichier de configuration d'exemple et modifiez-le selon vos besoins.

```
bash
Copier le code
cp etc/cowrie.cfg.dist etc/cowrie.cfg
nano etc/cowrie.cfg
```

Dans le fichier de configuration, vous pouvez ajuster plusieurs paramètres comme le port SSH (par défaut Cowrie utilise le port 2222) et le chemin des journaux.

8. Activer et lancer Cowrie

Vous pouvez maintenant démarrer Cowrie pour tester si tout fonctionne correctement.

```
bash
Copier le code
bin/cowrie start
```

Pour vérifier l'état de Cowrie :

```
bash
Copier le code
bin/cowrie status
```

9. Redirection du port 22 vers 2222

Par défaut, Cowrie écoute sur le port 2222 pour éviter les conflits avec le service SSH légitime. Si vous voulez que votre honeypot semble fonctionner sur le port 22 (par défaut pour SSH), il est nécessaire de rediriger le trafic réseau. Vous pouvez le faire avec `iptables`.

Tout d'abord, arrêtez le service SSH réel sur le port 22 :

```
bash
Copier le code
sudo systemctl stop ssh
```

Ensuite, redirigez le trafic du port 22 vers 2222 :

```
bash
Copier le code
sudo iptables -t nat -A PREROUTING -p tcp --dport 22 -j REDIRECT --to-port
2222
```

10. Configurer le démarrage automatique

Pour que Cowrie démarre automatiquement au démarrage du système, vous pouvez utiliser un script `systemd`. Créez un fichier de service systemd :

```
bash
Copier le code
sudo nano /etc/systemd/system/cowrie.service
```

Ajoutez les lignes suivantes :

```
bash
Copier le code
[Unit]
Description=Cowrie SSH Honeypot
After=network.target

[Service]
User=cowrie
WorkingDirectory=/home/cowrie/cowrie
ExecStart=/home/cowrie/cowrie/bin/cowrie start
ExecStop=/home/cowrie/cowrie/bin/cowrie stop
Restart=always

[Install]
WantedBy=multi-user.target
```

Ensuite, activez et démarrez le service Cowrie :

```
bash
Copier le code
sudo systemctl enable cowrie
sudo systemctl start cowrie
```

11. Vérifier les logs de Cowrie

Les journaux de Cowrie sont stockés dans le dossier `log`. Vous pouvez consulter les connexions et les activités des attaquants ici :

```
bash
Copier le code
cat log/cowrie.log
```

Conclusion

Vous avez maintenant un honeypot fonctionnel avec Cowrie sur Ubuntu 22.04.3. Vous pouvez surveiller les tentatives de connexion SSH et analyser le comportement des attaquants dans un environnement isolé. N’oubliez pas de surveiller régulièrement les journaux pour comprendre les attaques potentielles.

Si vous avez besoin de configurations plus avancées (comme des notifications d'attaques ou une intégration avec une solution SIEM), Cowrie offre également de nombreuses options de personnalisation.