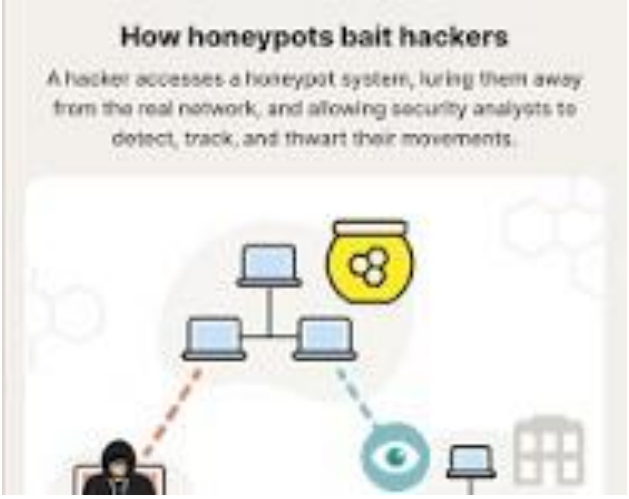


Année Scolaire : 2024/2025

Compte Rendu HoneyPort

Présenté par : Mathéo PAQUIN

Classe de SIO1A

Lycée Gustave Eiffel

SOMMAIRE

I.) Definition 3
Honeyport ou Pot de miel : 3
II.) Configuration du HoneyPort 3
III.) Enregistrement des tentatives de connexions et Capture des commandes qu'ils éxécutent 5

I.) Definition

Honeypot ou Pot de miel :

Le Honeypot ou le pot de miel est un programme conçu pour attirer les attaquants sur un port et cela permet aux équipes informatiques de surveiller les réponses de sécurité système et de le rediriger loin de la cible.

II.) Configuration du HoneyPot

Pour configurer notre HoneyPot la première chose a faire et de créer un fichier en python nommé honeyport.py.

Commande pour pouvoir le créer :

```
sudo nano honeyport.py
```

Puis quand on aura créer ce fichier, il faudra rentrer ce code qu'il va permettre de donner des alertes lorsque que l'attaquant saisi notre adresse IP sur le port 22 par exemple mon adresse IP de ma machine est 10.0.2.10

```python
import socket
import subprocess

PORT = 22  # Choisis ton port ici

def ban_ip(ip):
    print(f"[!] Connexion détectée depuis {ip} - Banni !")
    subprocess.call(['iptables', '-A', 'INPUT', '-s', ip, '-j', 'DROP'])

def start_honeyport():
    with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
        s.bind(('', PORT))
        s.listen(1)
        print(f"[+] Honeyport en écoute sur le port {PORT}")
        while True:
            conn, addr = s.accept()
            ip = addr[0]
            ban_ip(ip)
            conn.close()

if __name__ == "__main__":
    start_honeyport()
```

Quand ceci est fait, on va rendre le honeypot permanent donc il faudra créer un fichier nommé honeypot.service dans le chemin du dossier suivant puis on l'ouvre

```
sudo nano /etc/systemd/system/honeyport.service
```

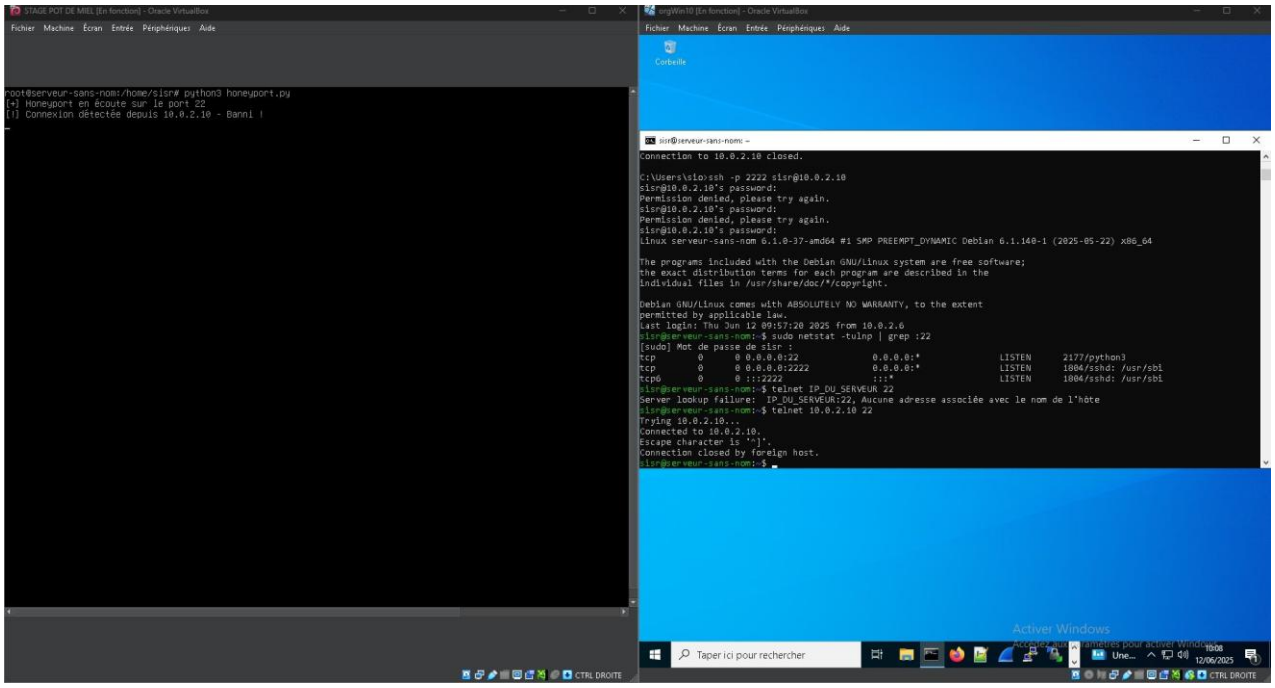
Puis on ouvre ce fichier et on va mettre le code suivant sur le fichier

```
[Unit]
Description=Honeyport piège
After=network.target

[Service]
ExecStart=/usr/bin/python3 /chemin/vers/honeyport.py
Restart=always

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

Puis on enregistre et on va activer les services dans l'image ci-dessous.

```
sudo systemctl daemon-reexec
sudo systemctl daemon-reload
sudo systemctl enable honeyport
sudo systemctl start honeyport
```

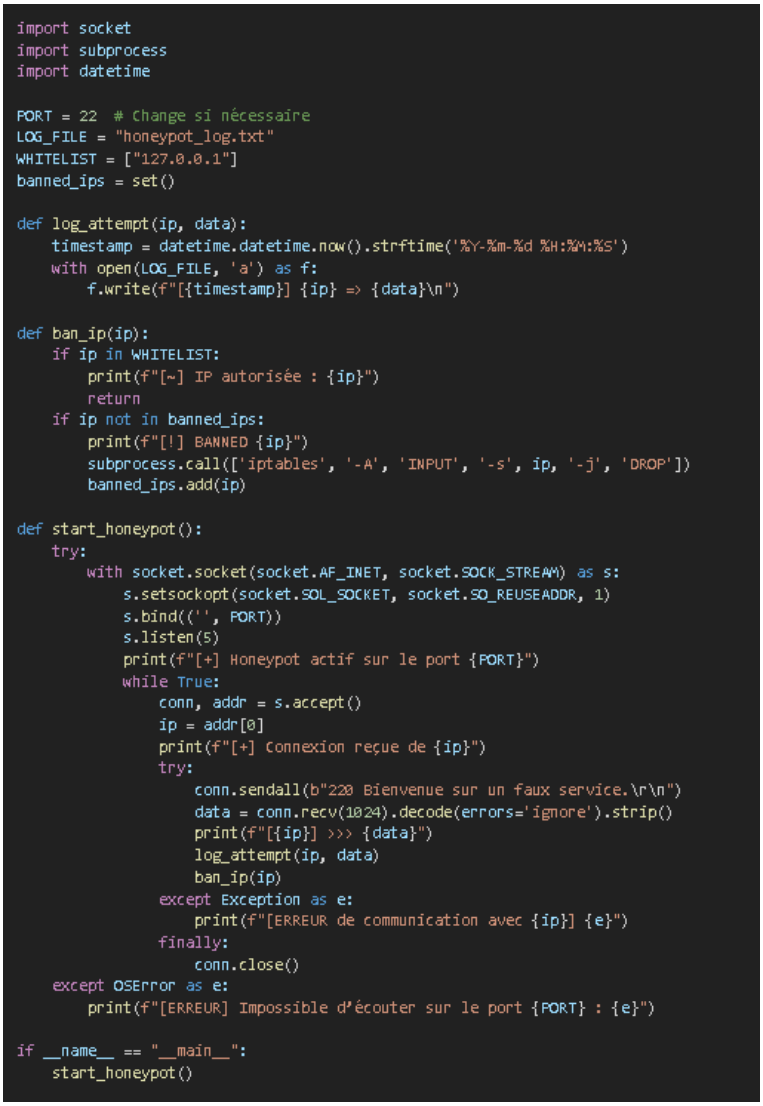
Et la on va lancer notre honeyport et taper sur une autre machine l'adresse IP pour voir si cela fonctionne et si cela fonctionne on devrait avoir ceci dans l'image ci-dessous.



III.) Enregistrement des tentatives de connexions et Capture des commandes qu'ils éxécutent

Maintenant on va essayer d'enregistrer les tentatives de connexions et de capturer les commandes que les attaquants peuvent exécuter.

Dans un premier temps on va modifier le fichier honeyport.py pour le remplacer par ce nouveau code qui permet justement que lorsque l'attaquant tape une commande qui renvoie un message par exemple de mon côté ca sera « Bienvenue sur un faux service »



```python
import socket
import subprocess
import datetime

PORT = 22  # Change si nécessaire
LOG_FILE = "honeypot_log.txt"
WHITELIST = ["127.0.0.1"]
banned_ips = set()

def log_attempt(ip, data):
    timestamp = datetime.datetime.now().strftime('%Y-%m-%d %H:%M:%S')
    with open(LOG_FILE, 'a') as f:
        f.write(f"[{timestamp}] {ip} => {data}\n")

def ban_ip(ip):
    if ip in WHITELIST:
        print(f"[~] IP autorisée : {ip}")
        return
    if ip not in banned_ips:
        print(f"[!] BANNED {ip}")
        subprocess.call(['iptables', '-A', 'INPUT', '-s', ip, '-j', 'DROP'])
        banned_ips.add(ip)

def start_honeypot():
    try:
        with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
            s.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
            s.bind(('', PORT))
            s.listen(5)
            print(f"[+] Honeypot actif sur le port {PORT}")
            while True:
                conn, addr = s.accept()
                ip = addr[0]
                print(f"[+] Connexion reçue de {ip}")
                try:
                    conn.sendall(b"220 Bienvenue sur un faux service.\r\n")
                    data = conn.recv(1024).decode(errors='ignore').strip()
                    print(f"[{ip}] >>> {data}")
                    log_attempt(ip, data)
                    ban_ip(ip)
                except Exception as e:
                    print(f"[ERREUR de communication avec {ip}] {e}")
                finally:
                    conn.close()
    except OSError as e:
        print(f"[ERREUR] Impossible d'écouter sur le port {PORT} : {e}")

if __name__ == "__main__":
    start_honeypot()
```

Puis quand cela est fait on va créer un fichier txt pour les logs que lorsque on va effectuer cette commande ca va nous montrer ce que l'attaquant à voulu essayer de taper avec le jour et la date.

Pour le créer :

```
touch honeypot_log.txt
```

Pour lui donner les droits :

```
chmod 666 honeypot_log.txt
```

On vérifie si cela a été bien crée :

```
ls -l honeypot_log.txt
```

```
-rw-rw-rw- 1 sisr sisr 0 juin 13 15:41 honeypot_log.txt
```

Quand cela est fait on teste le script avec cette commande :

```
sudo python3 honeypot.py
```

on tape n'importe quelle commande par exemple pour moi ca sera ceci :

```
nc 10.0.2.10 22
```

Quand vous avez tapé ceci vous aurez ceci dans l'image en dessous :

```
220 Bienvenue sur un faux service.
```

Puis pour voir les logs ca sera cette commande avec tout les détails en dessous de l'image :

```
cat honeypot_log.txt
```