

Reverse Shell

Reverse Shell en ASM x64

Lien : [https://github.com/DanielaCe18/
reverse-shell-asm](https://github.com/DanielaCe18/reverse-shell-asm)

Réalisé par : Daniela Ceraku



PLAN

01

Présentation Projet

02

Problématique

03

Fonctionnalités

04

Conception

05

Démonstration

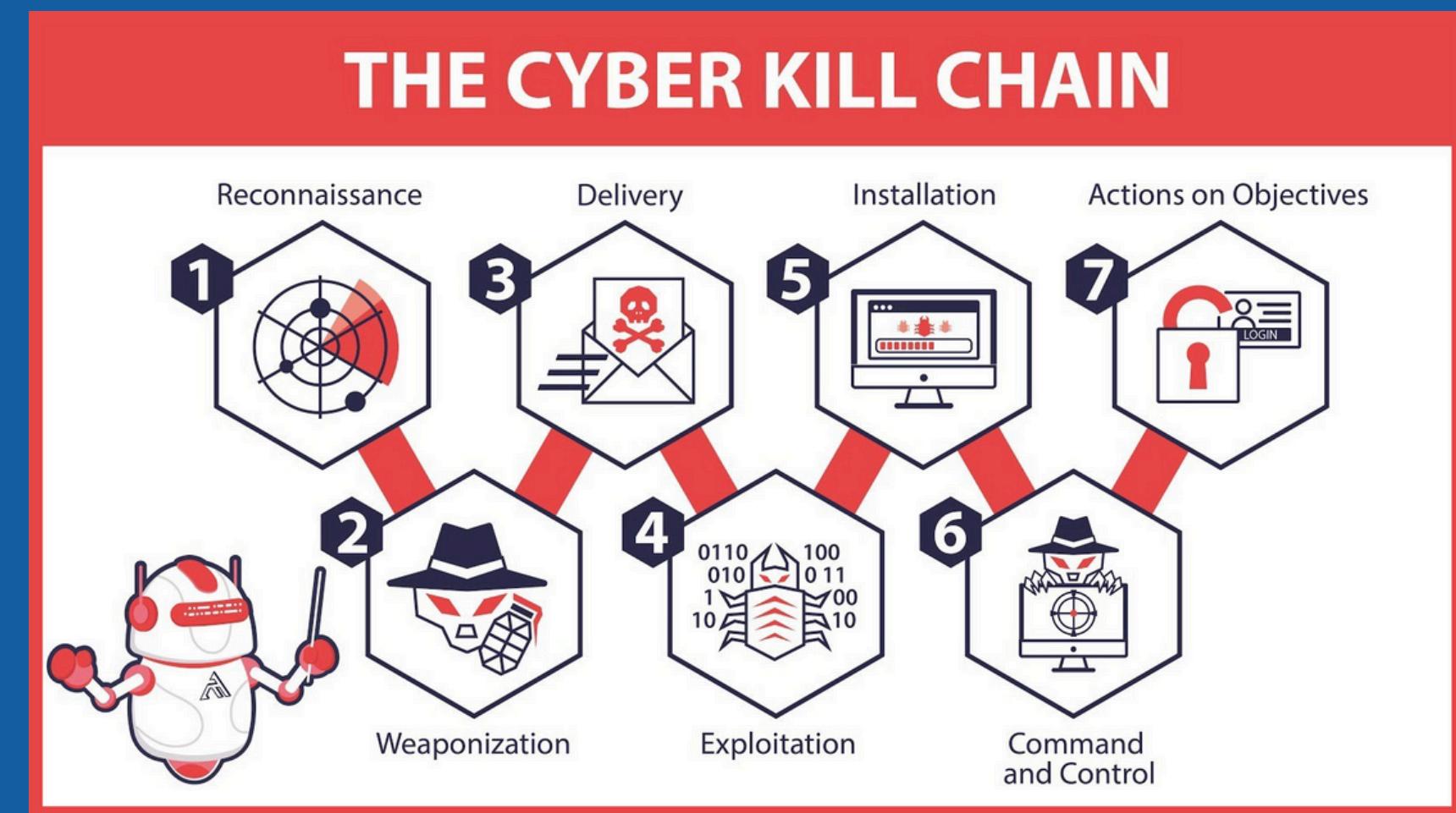
06

Perspectives



PROBLÉMATIQUE

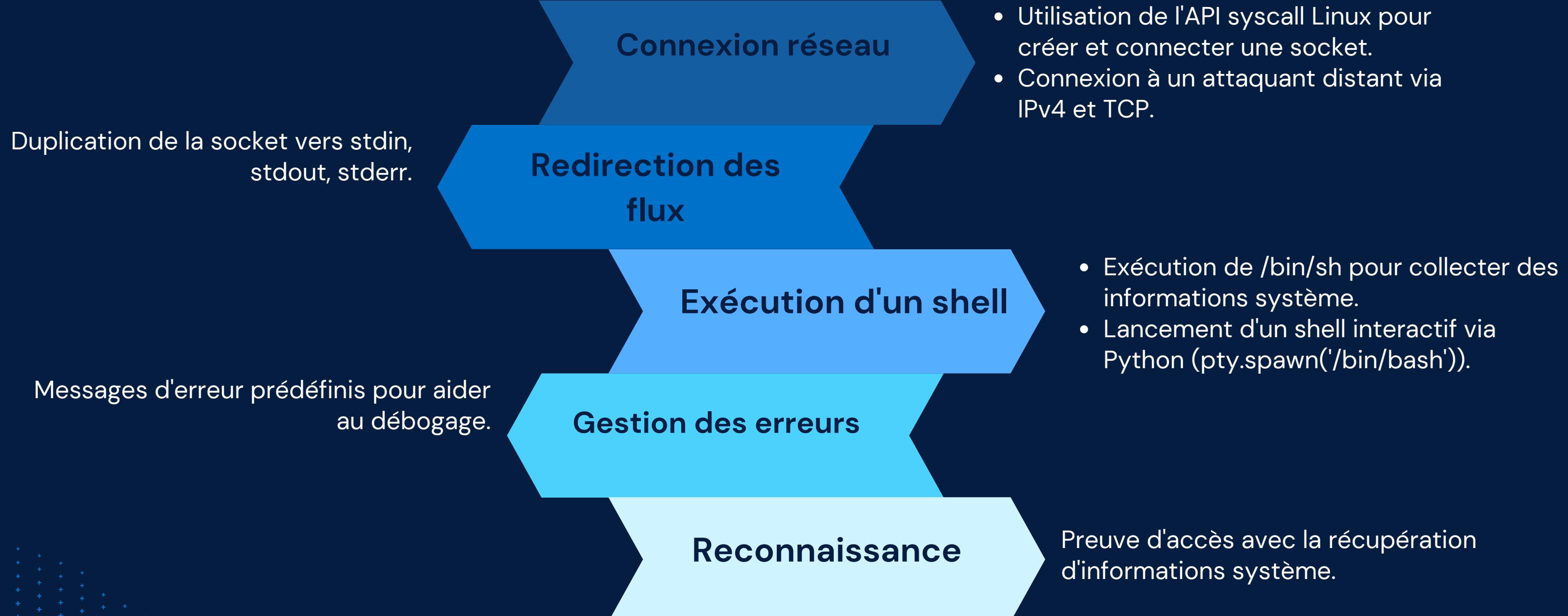
- Un reverse shell est un programme permettant d'établir une connexion inverse entre une machine cible et un attaquant.
- L'objectif est d'obtenir un accès distant à la machine cible en exploitant une communication sortante initiée par celle-ci.
- Ce projet consiste à implémenter un reverse shell en assembleur x86-64 afin de garantir un faible encombrement, une discréetion accrue et une exécution efficace.



CONCEPTION

- O1** Créer une socket en IPv4 et TCP.
Se connecter à une machine distante spécifiée (IP et port configurables).
- O2** Rediriger les entrées/sorties vers la socket afin d'exécuter des commandes à distance.
- O3** Utiliser execve pour exécuter un shell interactif (à travers Python3 pour garantir un environnement interactif).

FONCTIONNALITÉS





REVUE DU CODE ET DÉMONSTRATION



CONCLUSION

Perspectives

Encodage et obfuscation du binaire pour chiffrer les échanges.

Méchanismes anti-forensics en supprimant les preuves.

Bypass de l'EDR/firewall avec un reverse shell type ICMP.

Merci de votre attention

Daniela Ceraku

Lien : [https://github.com/DanielaCe18/
reverse-shell-asm](https://github.com/DanielaCe18/reverse-shell-asm)

