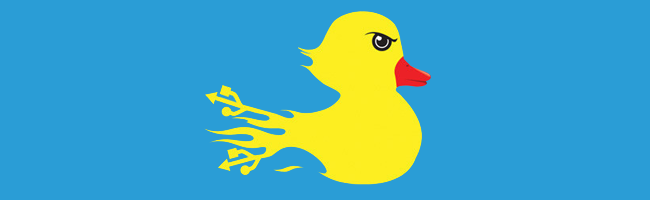
# Infecter un hôte

Pour infecter un hôte il faut avoir un accès physique à l’ordinateur et que la session sois ouverte.

Une fois que vous avez fait usage de votre meilleur social engineering pour distraire votre victime, il suffit de brancher votre clef USB rubber Ducky qui sera détecter comme un clavier.



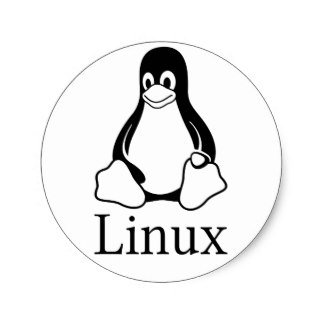
En quelques seconde seulement la DuckyDoor est installé.

# BUT

Avoir un programme léger qui permet de contrôler la machine serveur.

Le programme doit pouvoir télécharger / uploader des fichiers ainsi que d'exécuter des commandes.

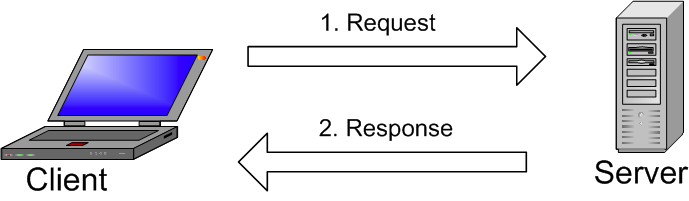
# Technologies



# Commandes Supportées

* ls Affiche le contenu du répertoire courant
* cd Change le répertoire courant
* mkdir Crée un dossier
* get Télécharge un fichier
* put Envoie un fichier sur le serveur
* exec Exécute une commande
* keylog Démarre la capture d’input
* exit Ferme la connexion
* help Affiche la liste des commandes

# Architecture



# Fonctionnement

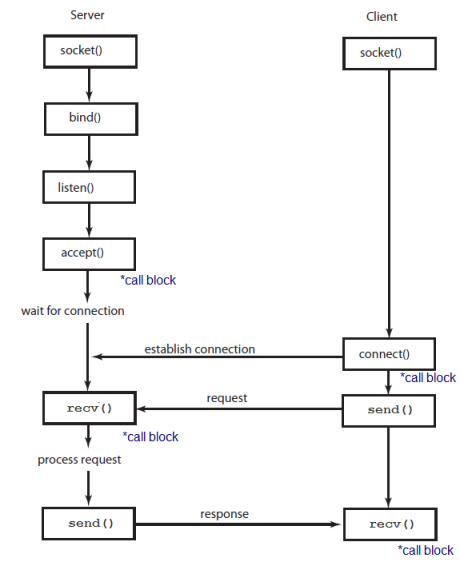
Une fois votre hôte infecté, il est possible de se connecter à la DuckyDoor via son adresse IP.

La communication se fait par python et sa lib. Socket.

C’est désormais à vous de jouer en utilisant les commandes supportées

# Socket

1. Le serveur attend une connexion
2. Le client se connecte à se port
3. Une connexion est alors créée et permet de communiquer



DuckyDoor

Une backdoor avec python