







## : Principe de fonctionnement

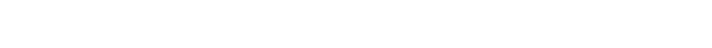




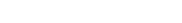






























## pedirection de port



# Exploitation

# Contournement de pare-feu

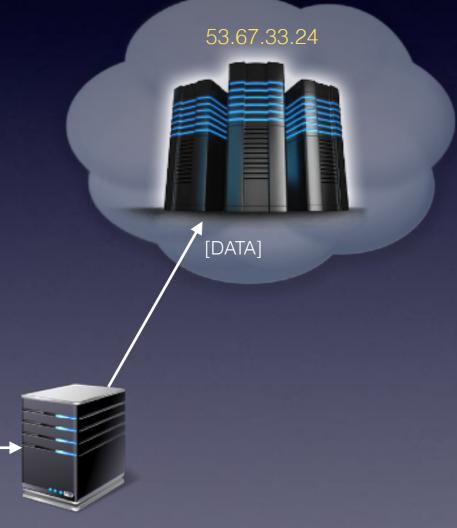
pedirection de port : Principe de fonctionnement

1 : L'attaquant configure le mécanisme de rebond sur le serveur : Port à écouter, Adresse IP de destination, Port de destination. Ex : tout ce qui arrivera sur 4444/TCP sera renvoyé vers 53.67.33.24:80

2 : Le client réalise une connexion sur le port 4444/TCP du serveur

3 : Le serveur accepte la connexion TCP et établit une nouvelle connexion vers la machine 53.67.33.24 sur 80/TCP

4 : Dès lors, toutes les informations qui arrivent du client (cnx 1) sont renvoyées automatiquement sur l'autre connexion (cnx 2)







# Exploitation

# Contournement de pare-feu

Rebonds: redirection de port

## Avantages:

 Les communications à destination de www.entreprise.net proviennent du serveur et non de la machine cliente.

## Inconvénients:

- Nécessite une configuration au préalable de la machine de transfert;
- Le transfert est limité à une seule adresse IP ;
- La confidentialité des communications repose sur la connexion à transférer.