SYNACKTIV

# SOCKSQLmap

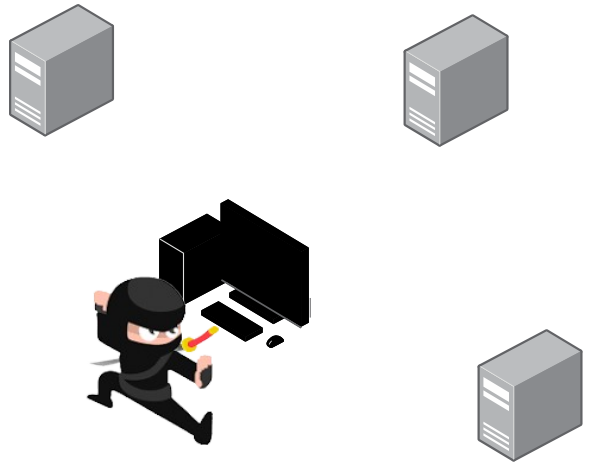
## The Network bootcamp

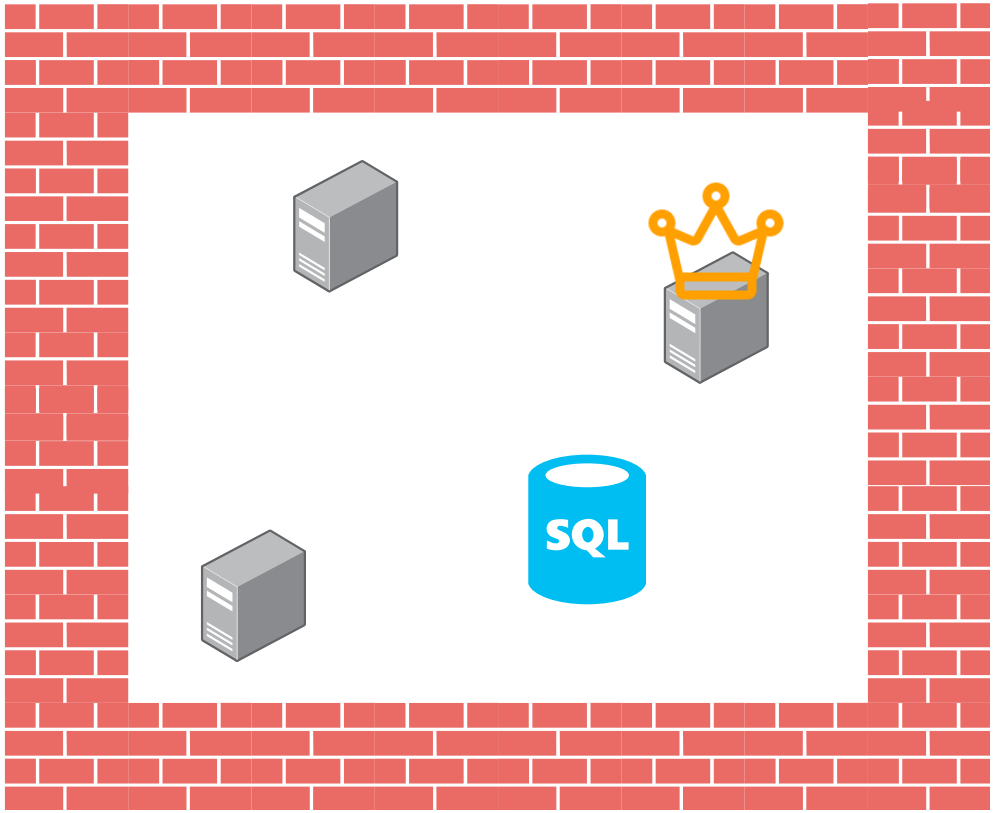
Meet-up TSP & IPP - @_bluesheet

24/10/2024

# Contexte

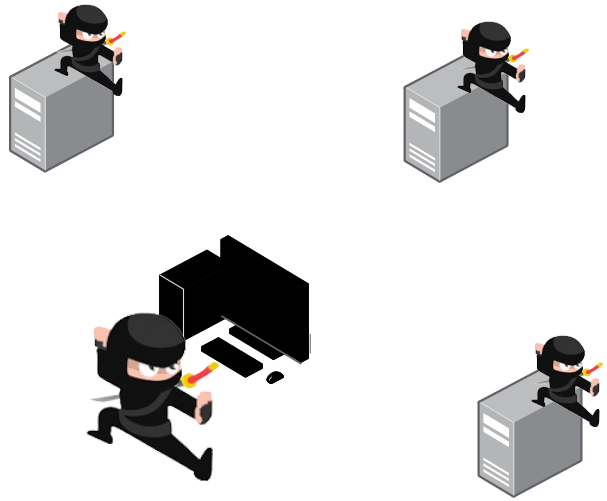
SYNACKTIV

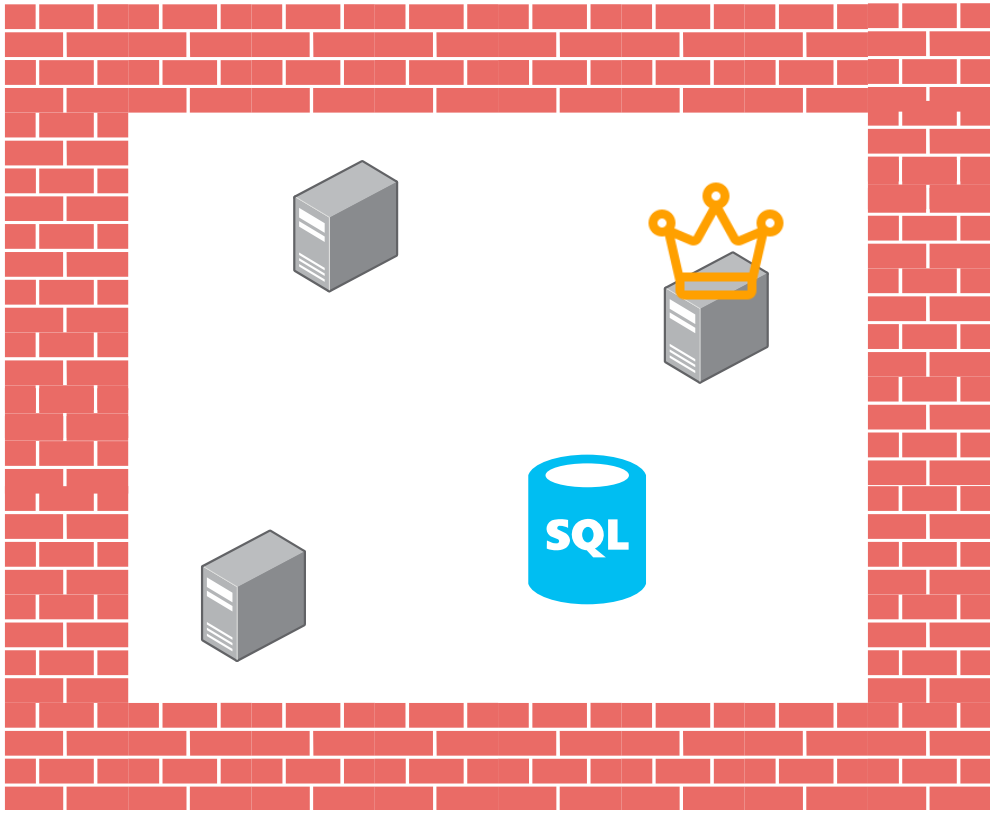




# Contexte

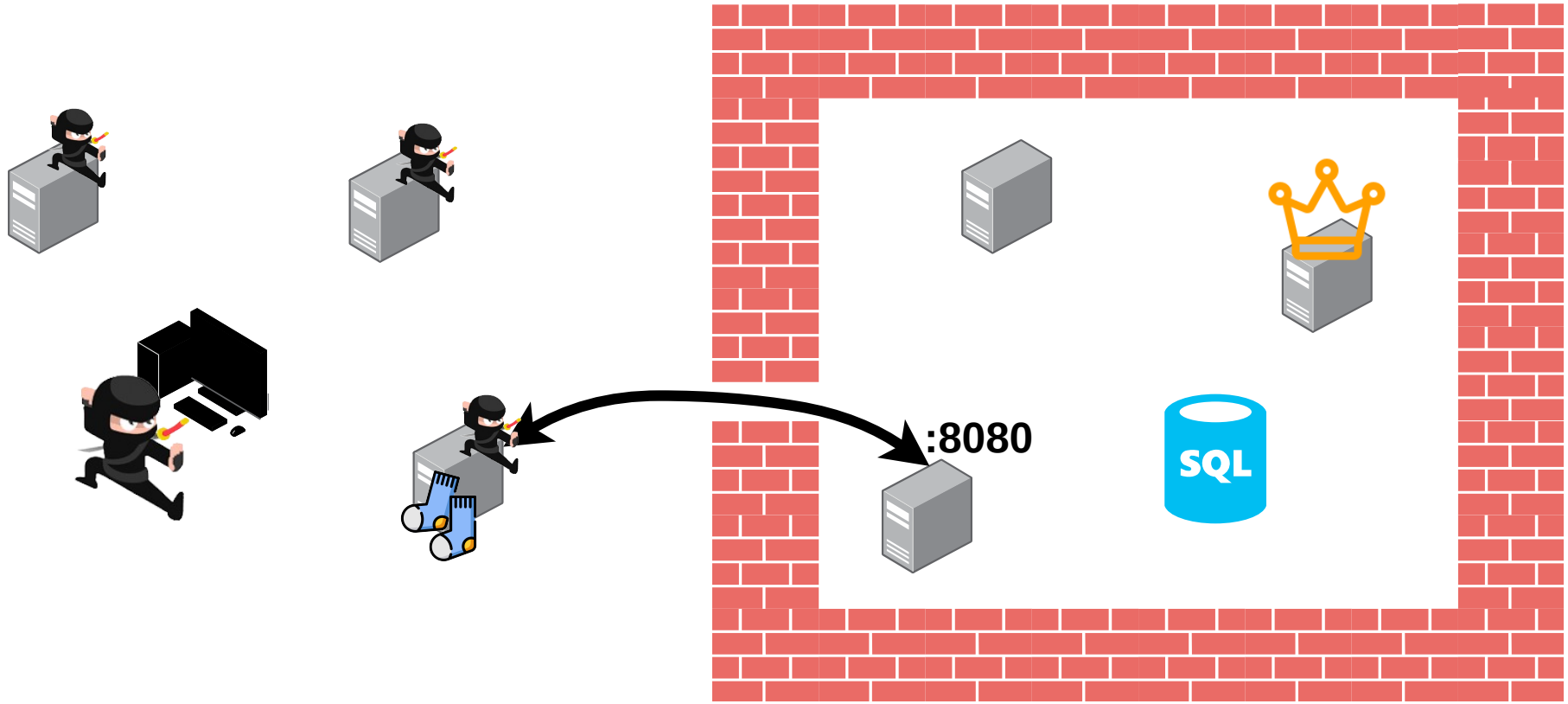
SYNACKTIV





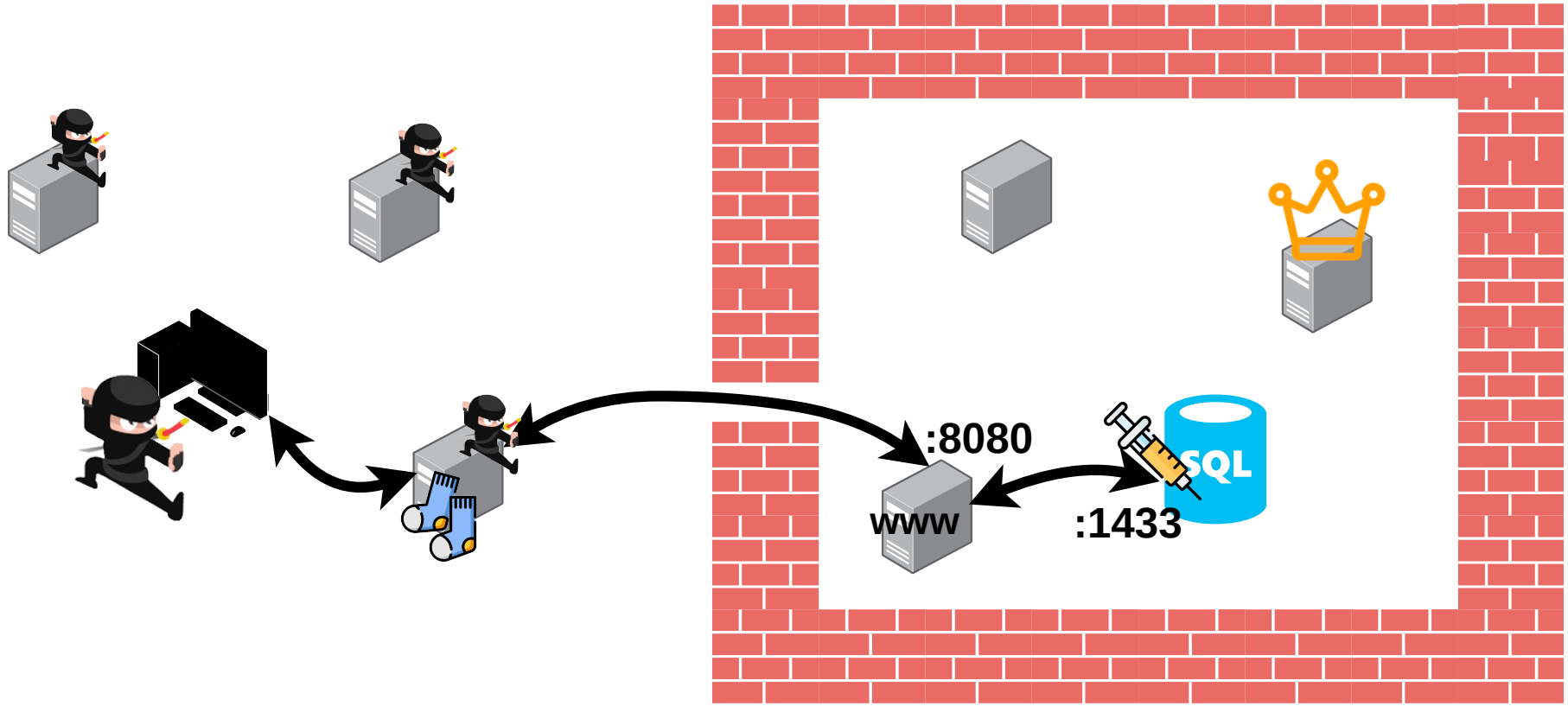
# Contexte

SYNACKTIV



# Contexte

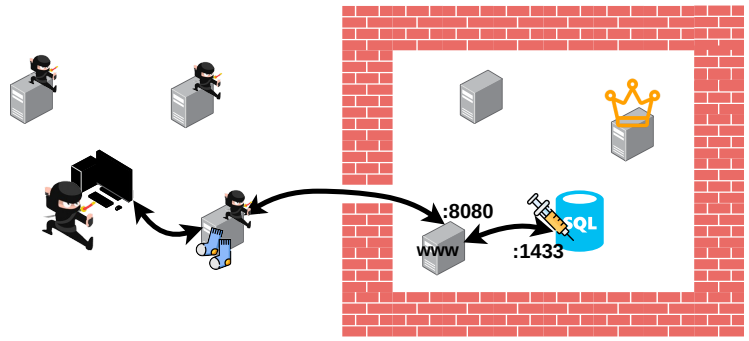
SYNACKTIV



# Contexte

SYNACKTIV

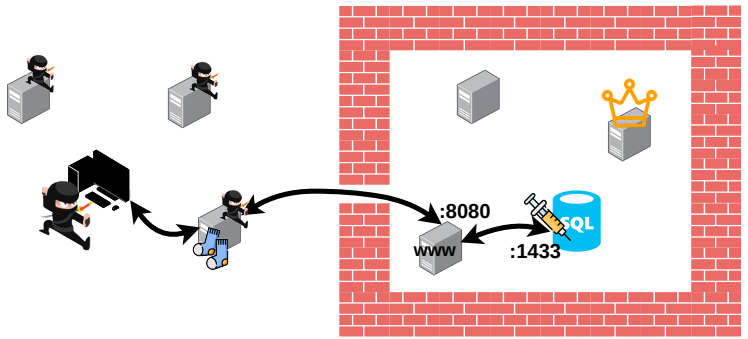
- **Injection SQL, MSSQL edition**
  - Utilisateur **`sa`**
  - xp_cmdshell → RCE
  - `sqlmap --os-shell` 👍
- **Compromission de la DB → Pivot réseau ?**
  - Pas de communications directes avec la DB
  - Serveur web intermédiaire pas compromis
  - Ne sort pas sur internet (même pas en DNS)



# SOCKS ?

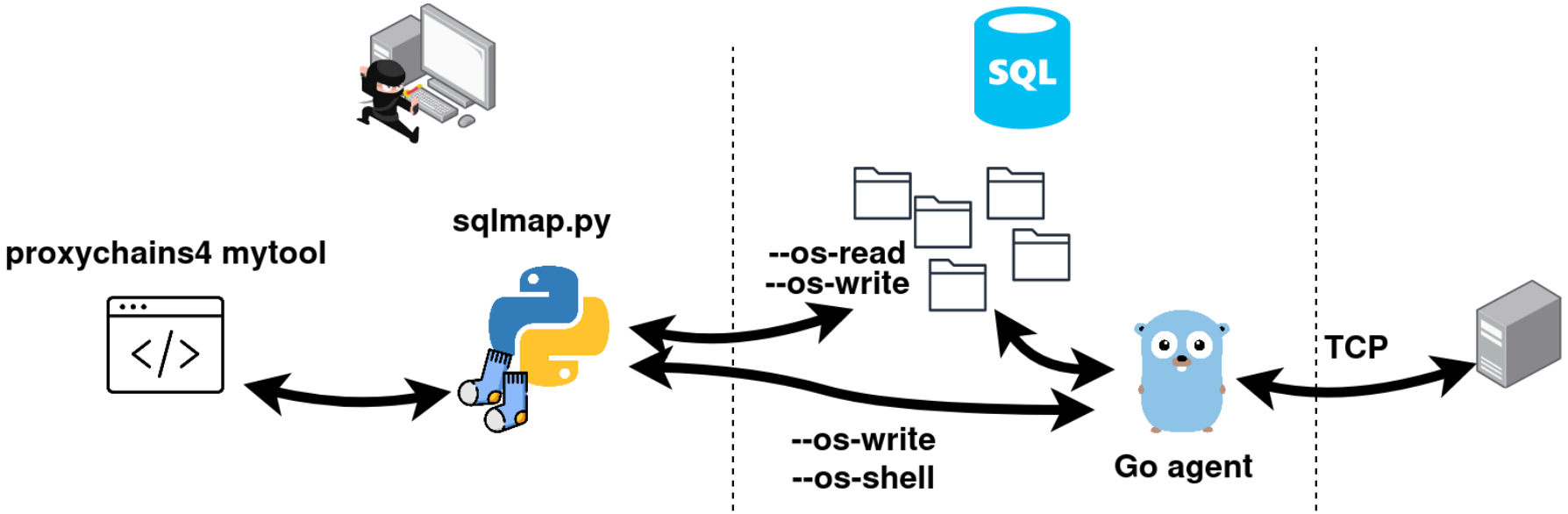
SYNACKTIV

- **Un serveur SOCKS sans réseau ?**
  - Émuler une socket TCP avec la RCE
  - File read/write, possible avec SQLmap (`--os-read` / `--os-write` / `--os-shell`)



# SOCKSQLmap

SYNACKTIV



# SOCKSQLmap

SYNACKTIV

1. C → S : `uid_dstaddr_dstport_open.socks`
2. S → C : `uid_dstaddr_dstport_openstatus.socks`
3. C → S : `uid_dstaddr_dstport_tx_1.socks`
4. C → S : `uid_dstaddr_dstport_tx_2.socks`

...

59. S → C : `uid_dstaddr_dstport_rx_1.socks`

...

684. S → C / C → S : `uid_dstaddr_dstport_close.socks`

# SOCKSQLmap

SYNACKTIV

- **Les +**
  - Pas limité à SQLmap, SOCKS générique à partir d'une RCE
  - Exercice sympa
  - Client compréhensif, fournit un accès propre après le POC
- **Les -**
  - C'est **LENT**
  - Pas très pratique avec SQLmap, il faut compiler le Go pour l'archi de la DB en avance

# Synacktiv recrute ! 😉

SYNACKTIV

https://www.linkedin.com/company/synacktiv

https://twitter.com/synacktiv

https://synacktiv.com