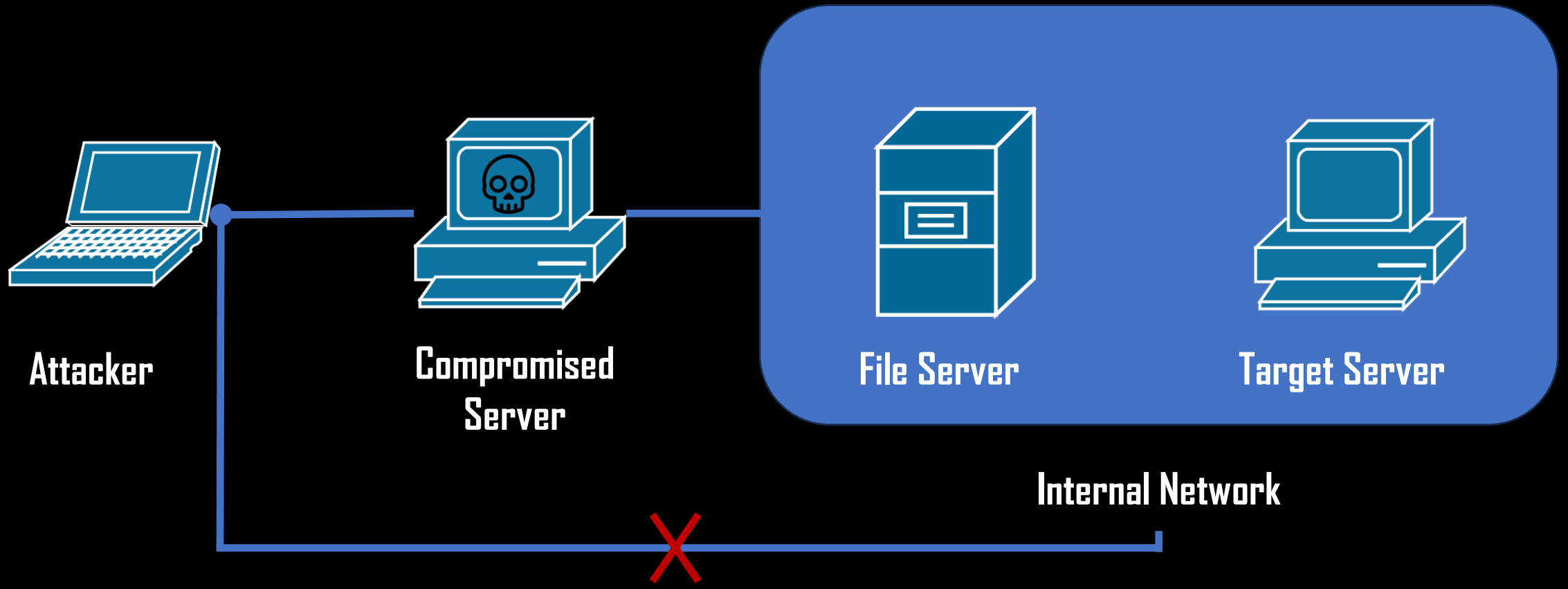
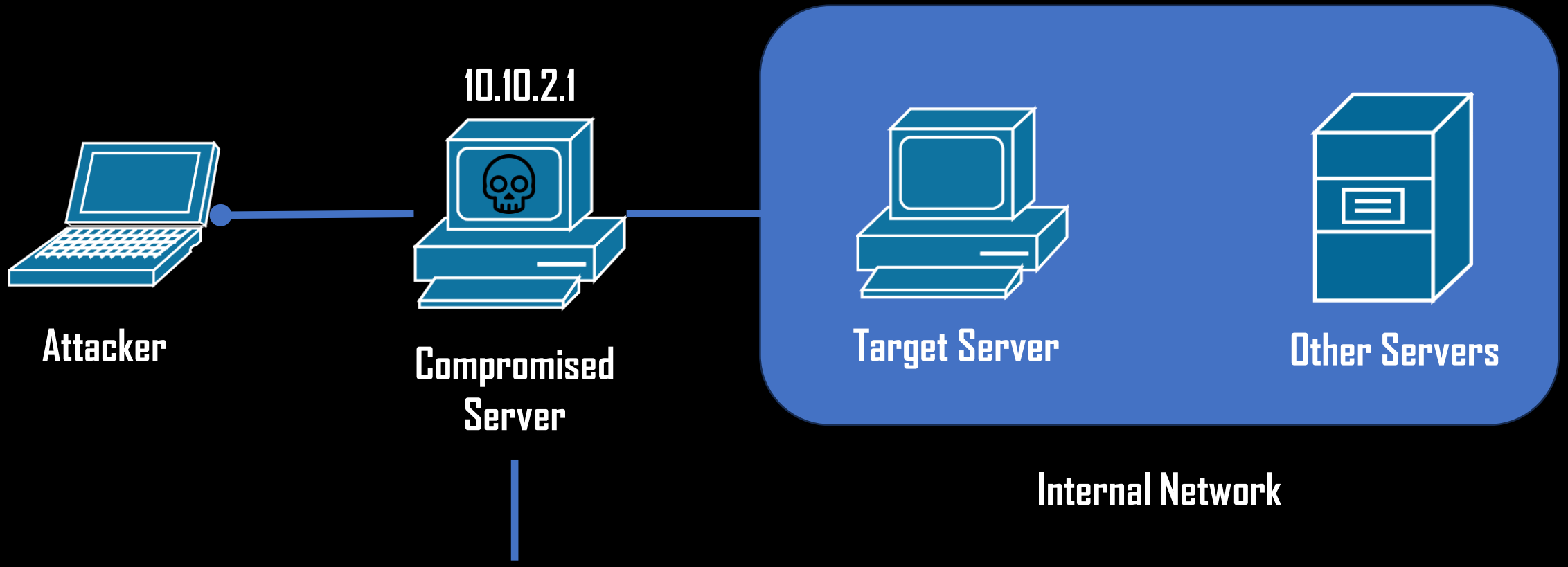
SSH Port Forwarding

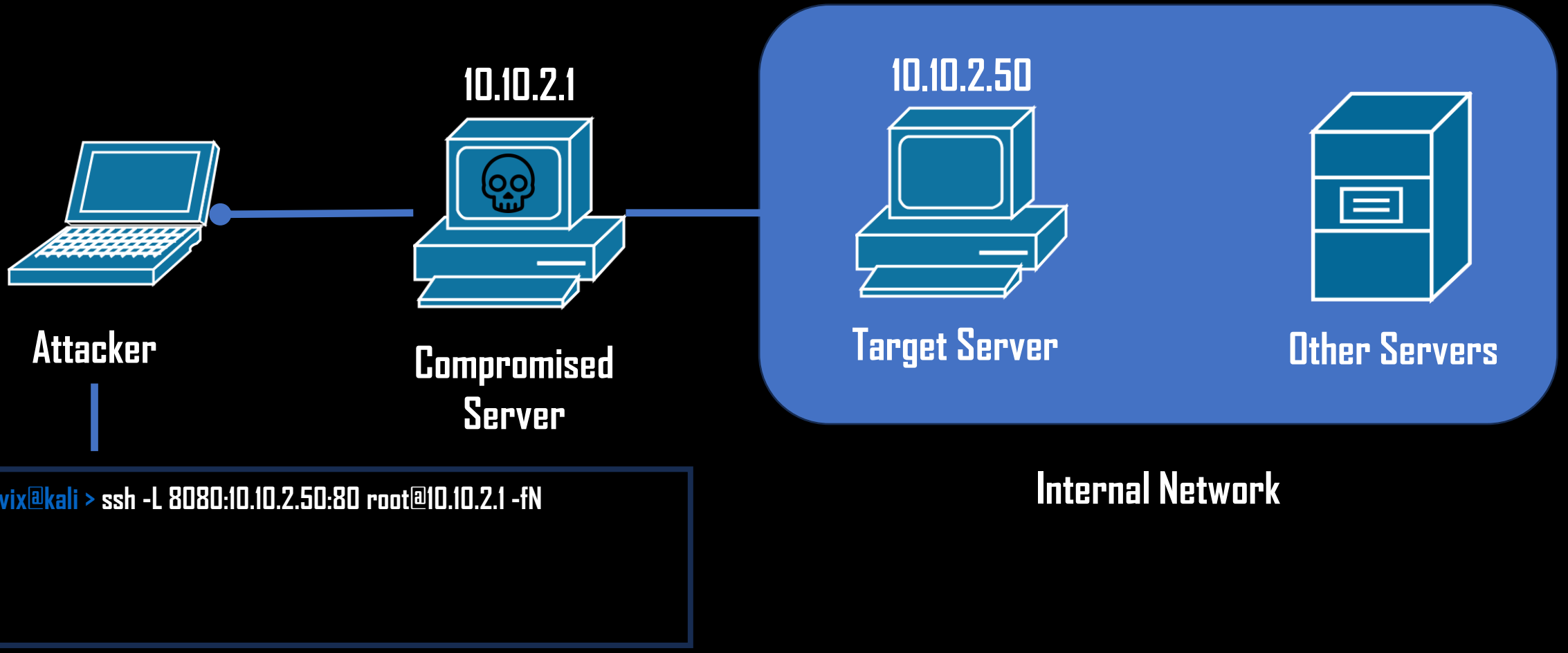


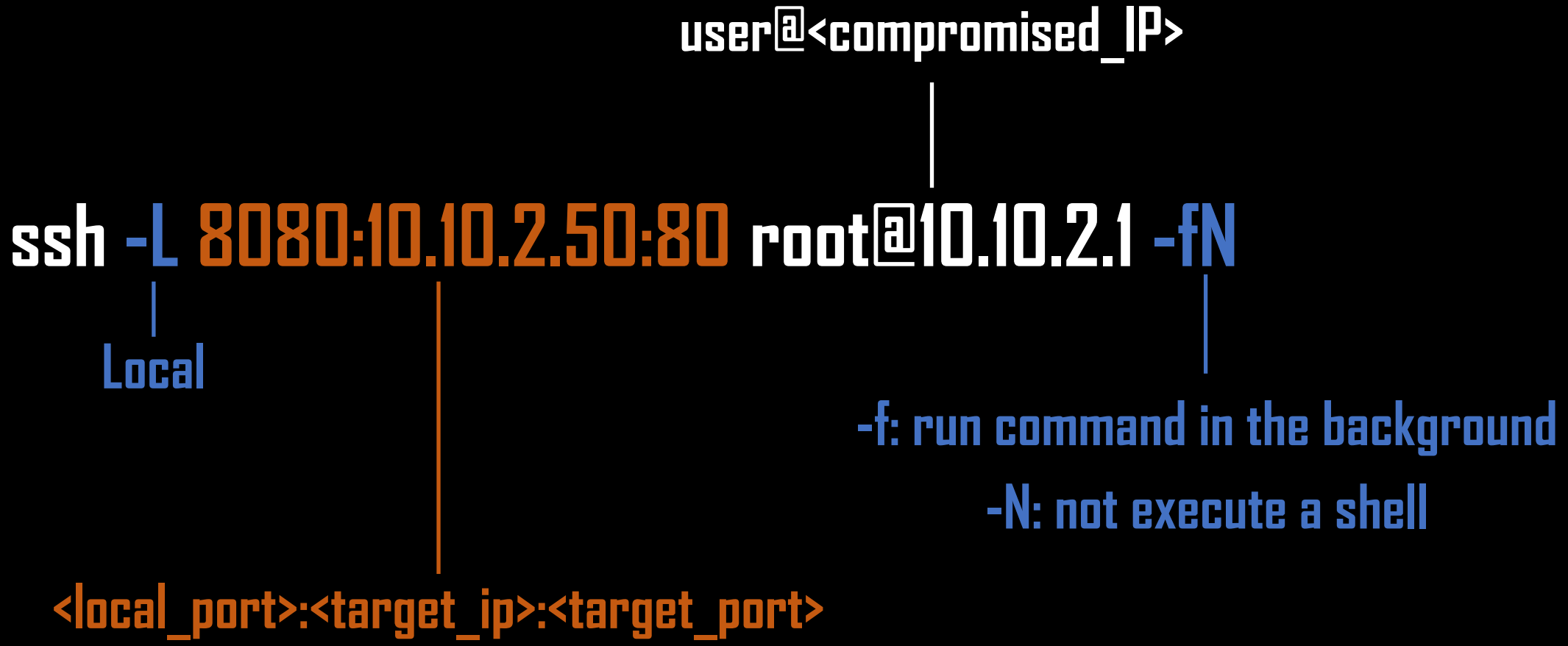


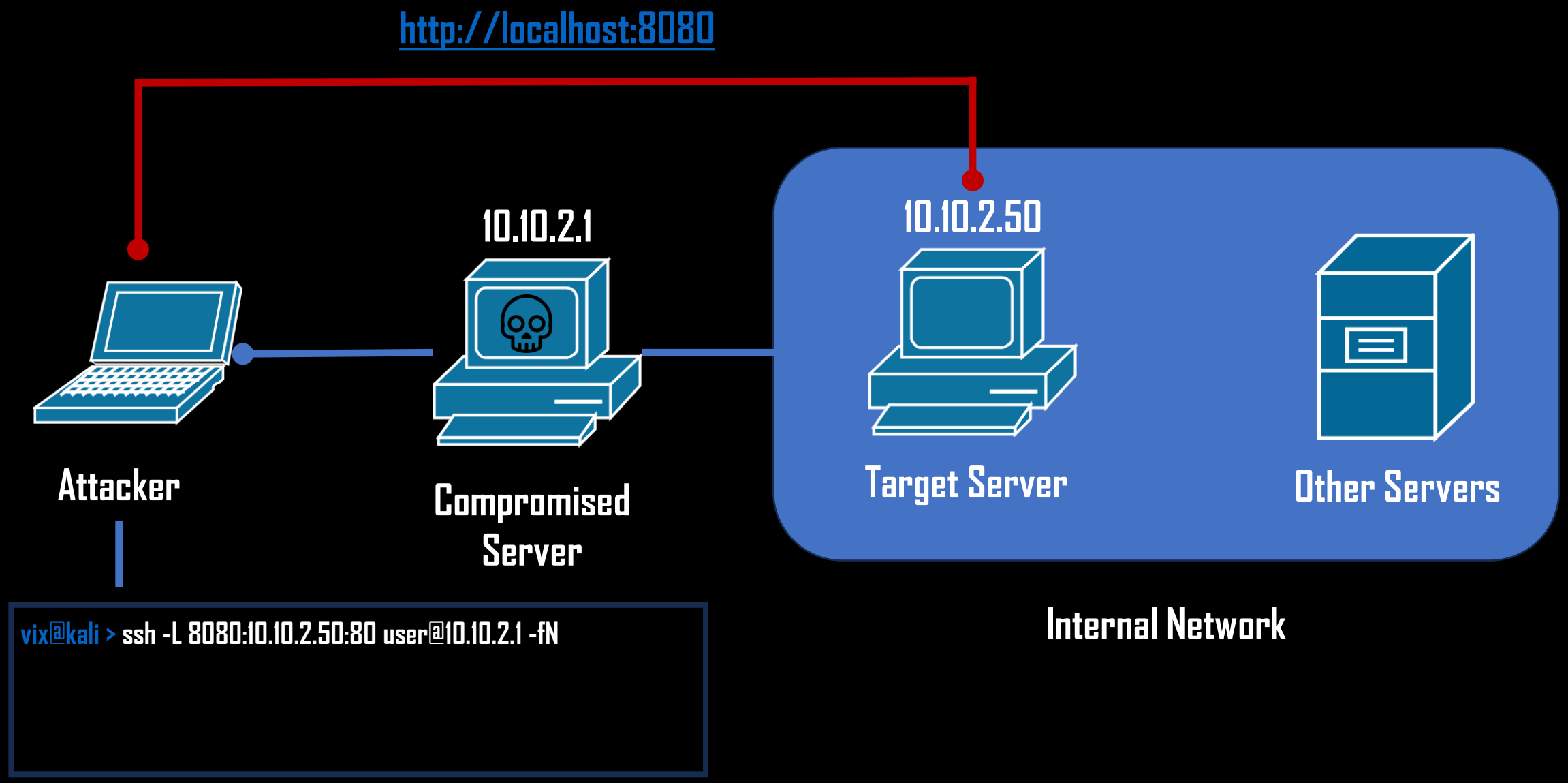

```
root@10.10.2.1 > ./nmap –sn 10.10.2.0/24  --exclude  10.10.2.1
Nmap scan report for 10.10.2.50
Host is up (0.0015s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
```

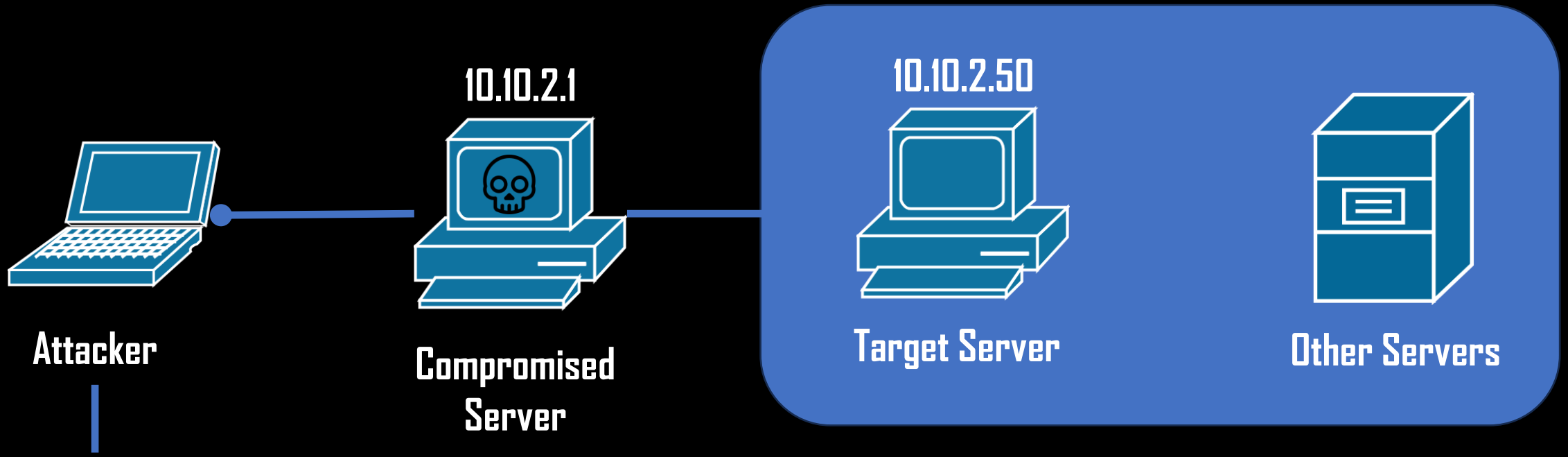
Local Forwarding



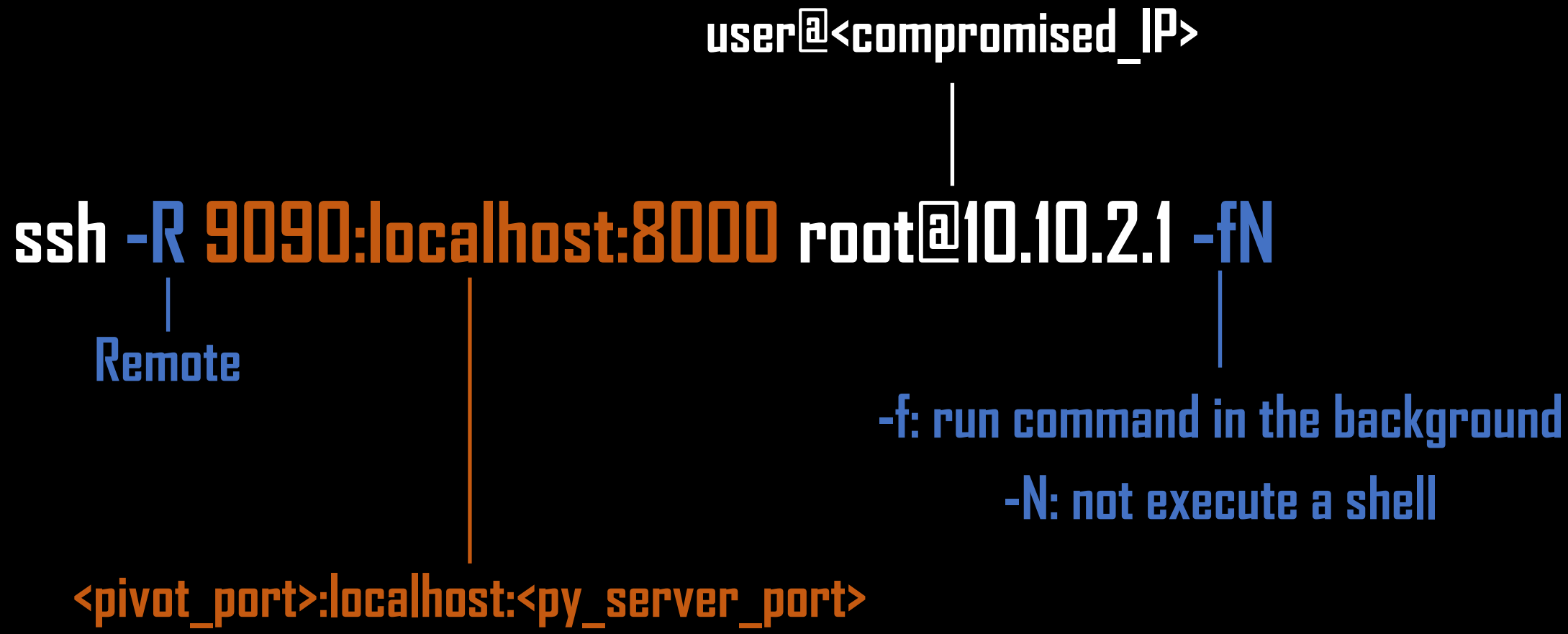

user@<compromised_IP>
ssh -L 8080:10.10.2.50:80 root@10.10.2.1 -fN
Local
<local_port>:<target_ip>:<target_port>
-f: run command in the background
-N: not execute a shell

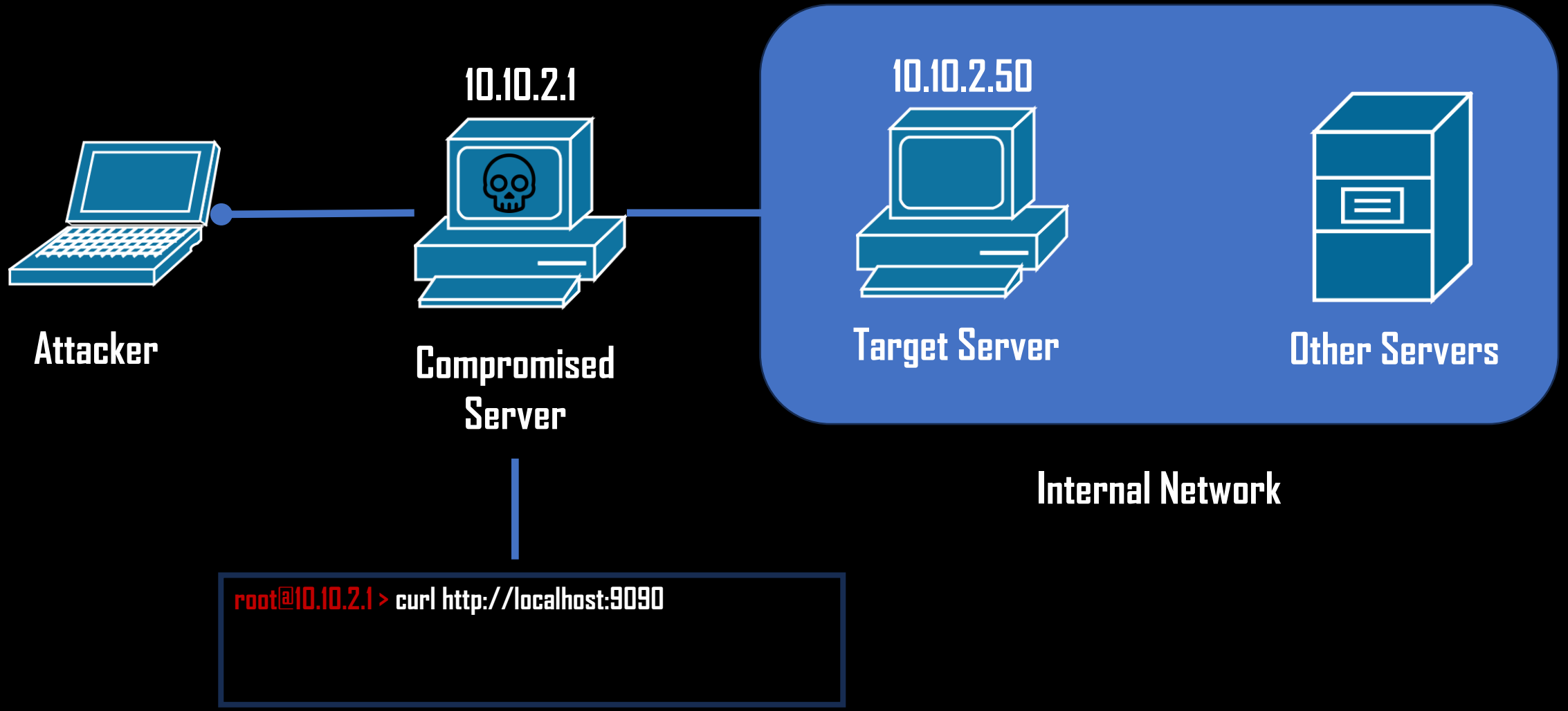

http://localhost:8080
10.10.2.1
10.10.2.50
Attacker
Compromised Server
Target Server
Other Servers
vix@kali > ssh -L 8080:10.10.2.50:80 user@10.10.2.1 -fN
Internal Network

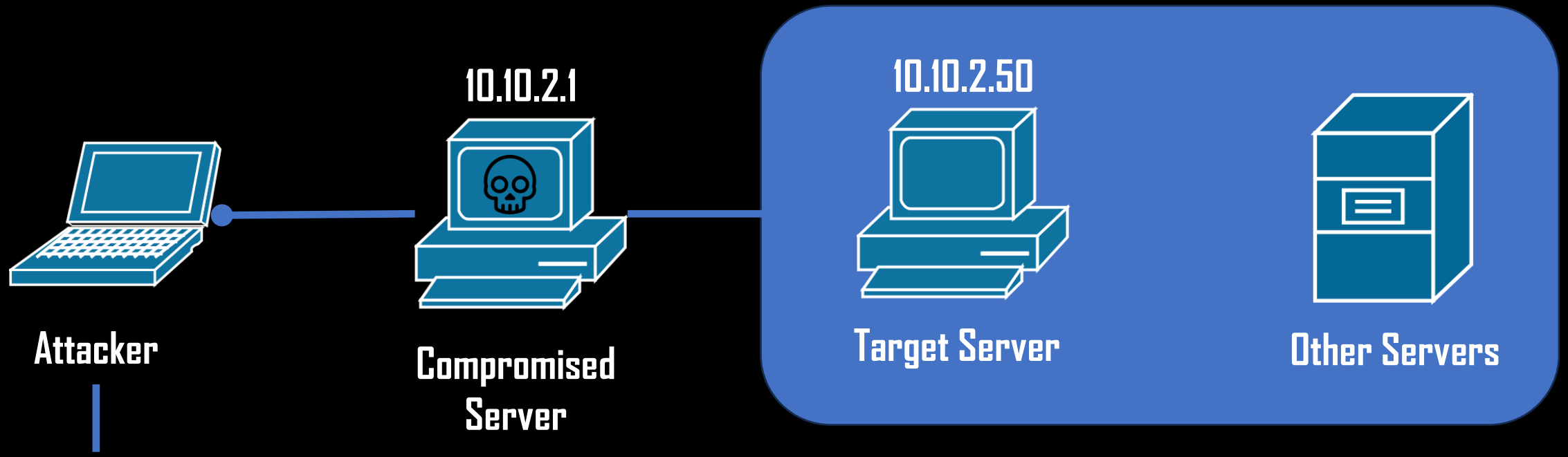
Remote Forwarding/Reverse Connection




```
vix@kali > python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
--------------------------------------------------------------------------------
vix@kali > ssh -R 9090:localhost:8000 user@10.10.2.1 -fN
```


user@<compromised_IP>
ssh -R 9090:localhost:8000 root@10.10.2.1 -fN
Remote
-f: run command in the background
-N: not execute a shell
<pivot_port>:localhost:<py_server_port>


10.10.2.1
10.10.2.50
Attacker
Compromised Server
Target Server
Other Servers
Internal Network
root@10.10.2.1 > curl http://localhost:9090




```
vix@kali > python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
127.0.0.1 - - [8/Jul/2025 12:15:30] "GET / HTTP/1.1" 200 -
--------------------------------------------------------------------------------
vix@kali > ssh -R 9090:localhost:8000 user@10.10.2.1 -fN
```