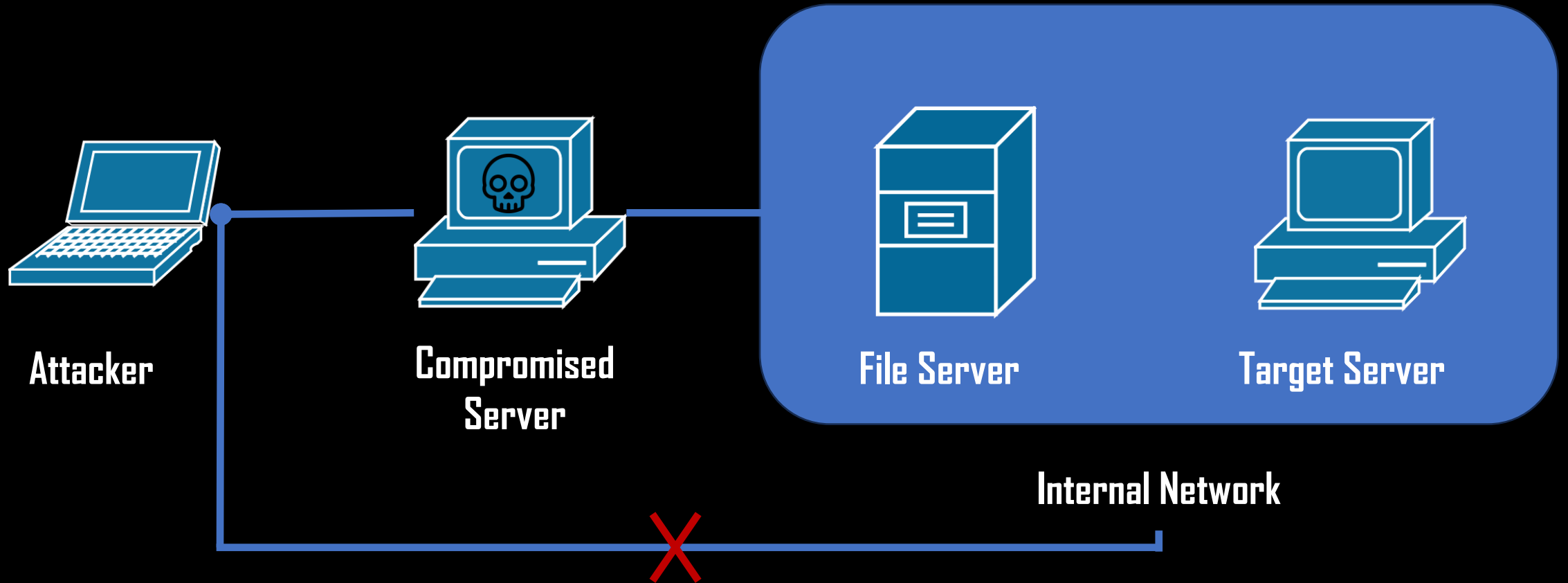
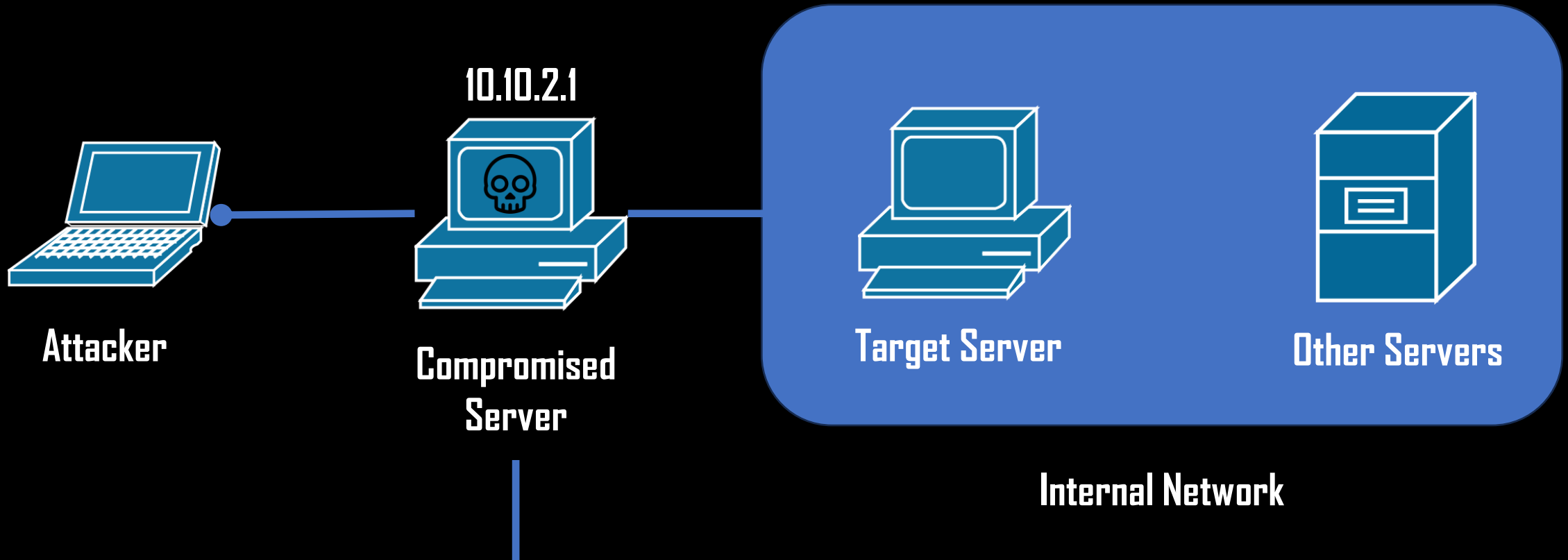


# SSH Port Forwarding





```
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
```

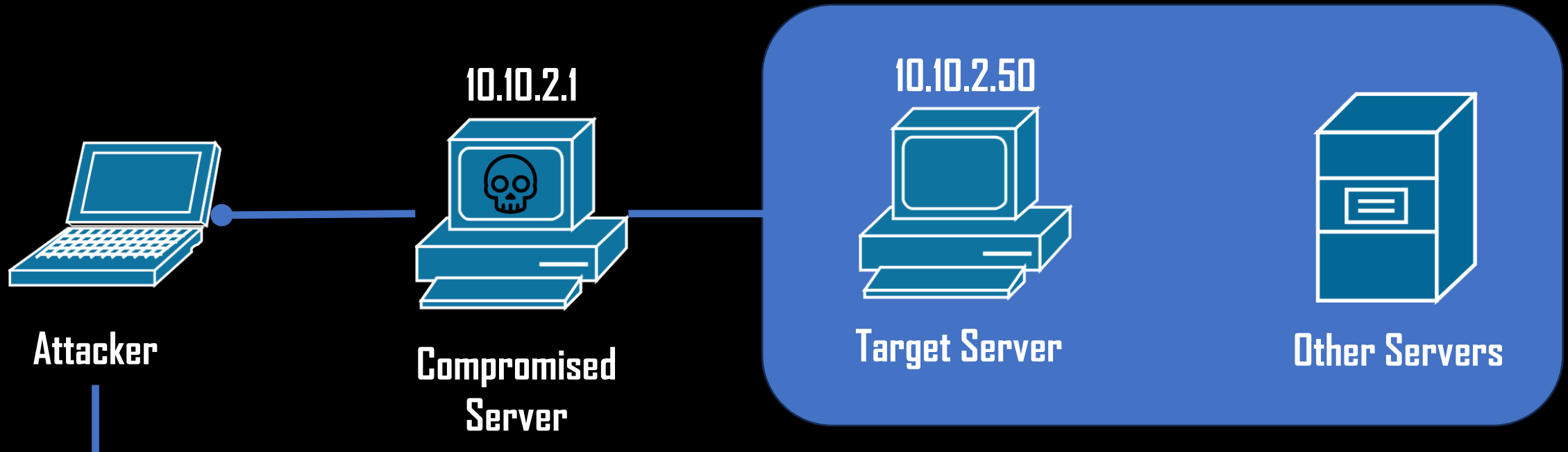
```
Host is up (0.0015s latency).
```

```
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



Internal Network

```
vix@kali > ssh -L 8080:10.10.2.50:80 root@10.10.2.1 -fN
```

user@<compromised\_IP>

ssh -L 8080:10.10.2.50:80 root@10.10.2.1 -fN

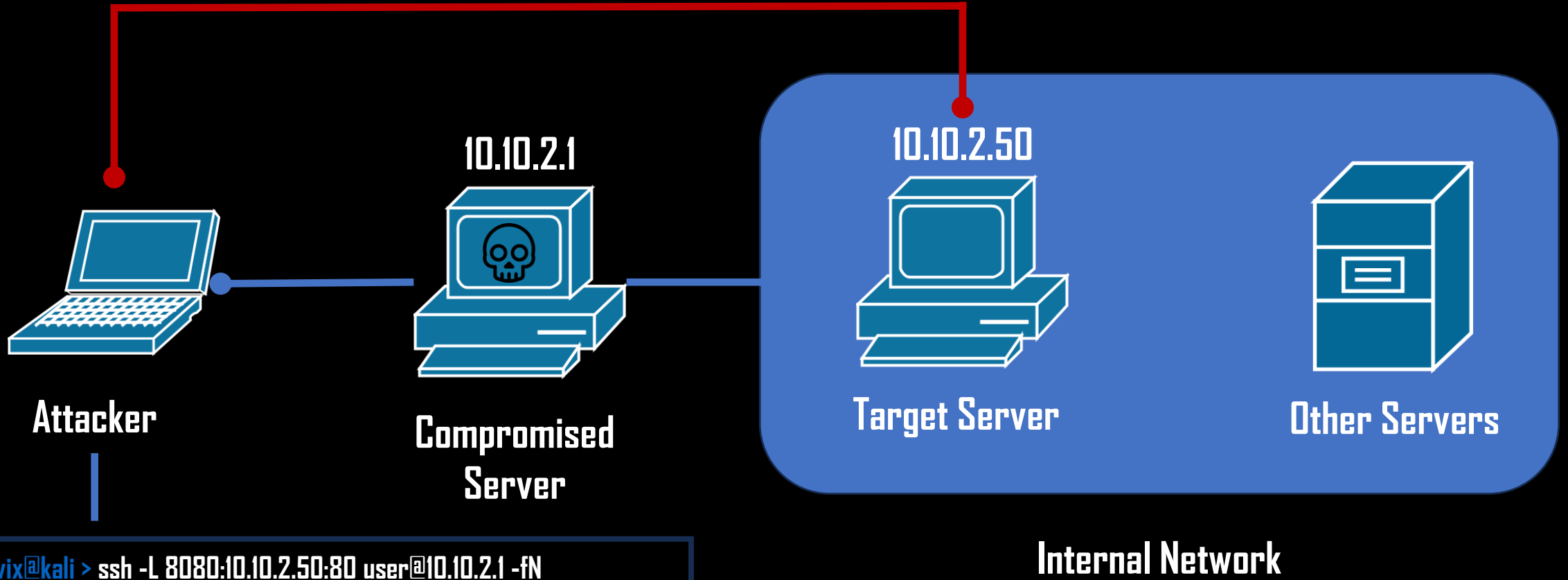
Local

-f: run command in the background

-N: not execute a shell

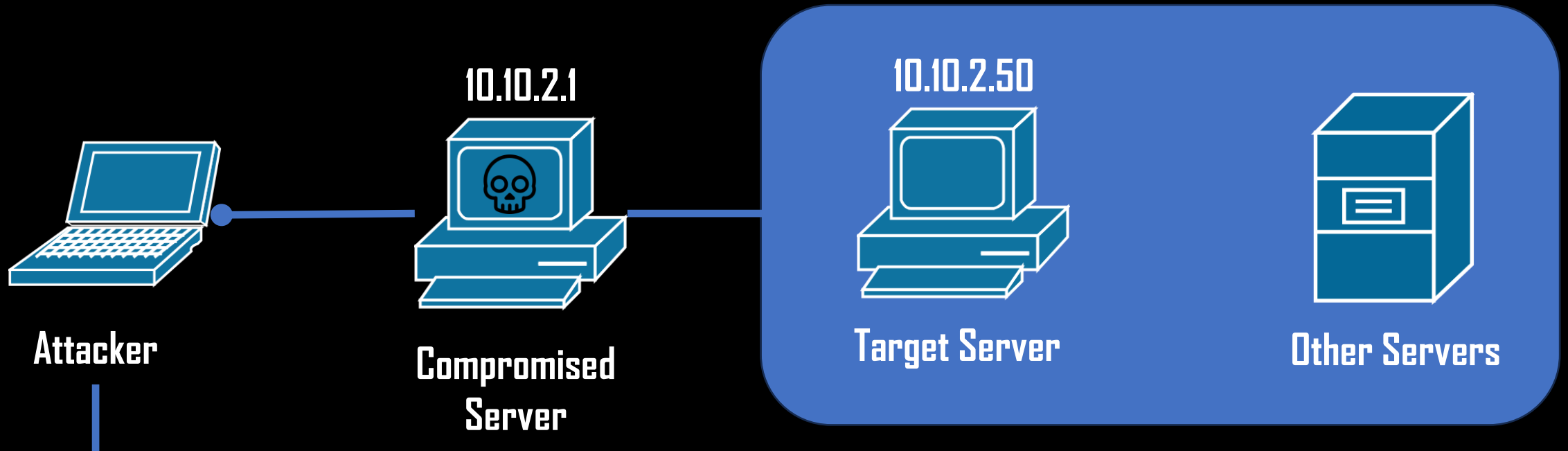
<local\_port>:<target\_ip>:<target\_port>

<http://localhost:8080>



```
vix@kali > ssh -L 8080:10.10.2.50:80 user@10.10.2.1 -fN
```

# 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>

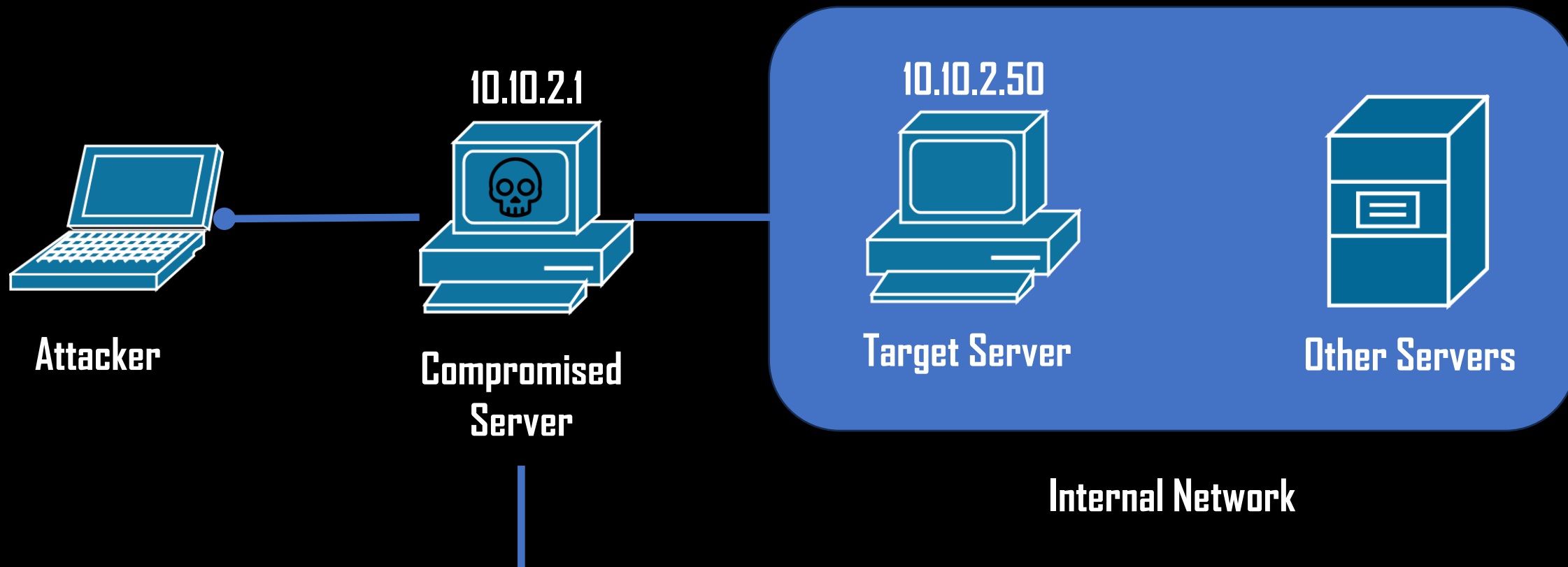
ssh -R 9090:localhost:8000 root@10.10.2.1 -fN

Remote

-f: run command in the background

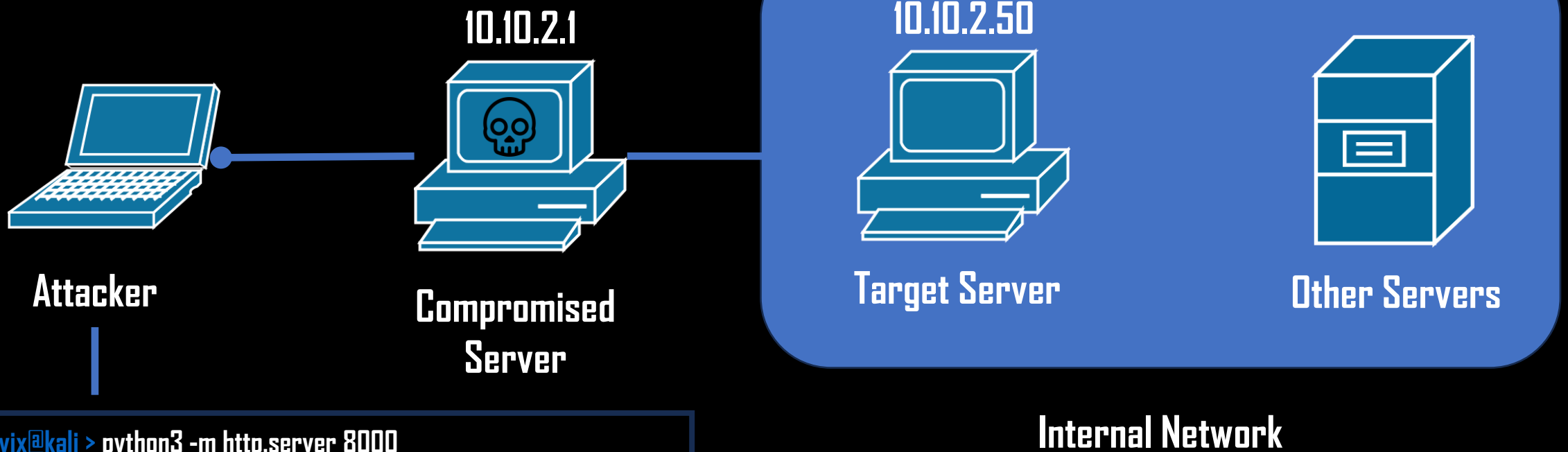
-N: not execute a shell

<local\_port>:localhost:<py\_server\_port>



```
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
```