

# Defense Evasion with ProxyChains

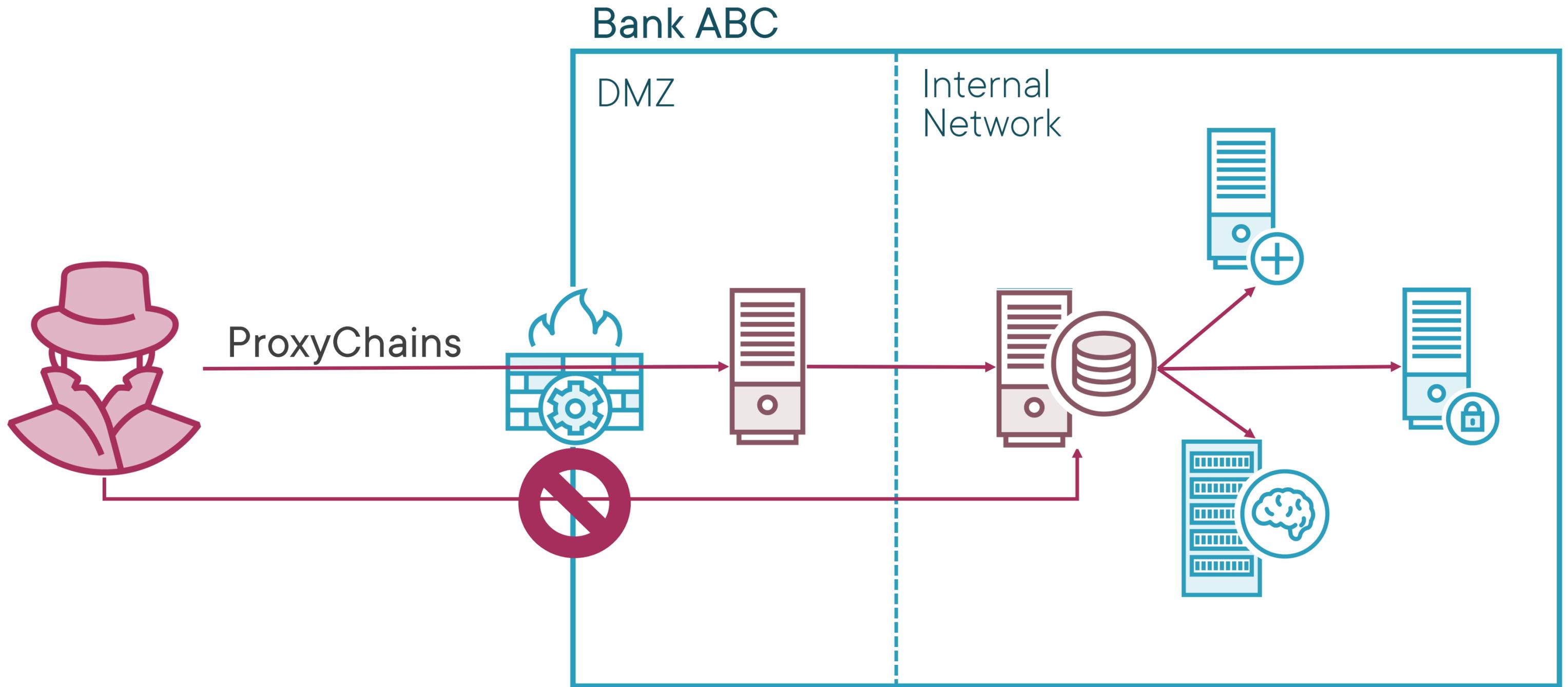
---



**Ricardo Reimao, OSCP, CISSP**  
Cybersecurity Consultant



# Bypassing Network Perimeter Defense



# ProxyChains



# ProxyChains

**Creator:** N3E7CR34TUR3

**Main Contributors:** rofl0r, Adam Hamsik and Jianing Yang

---

A tool that forces any TCP connection made by any given application to follow through proxy like TOR or any other SOCKS4, SOCKS5 or HTTP(S) proxy.



# ProxyChains

**Open source software**

**<https://github.com/haad/proxychains>**

**One of the most well known tools for traffic redirection**

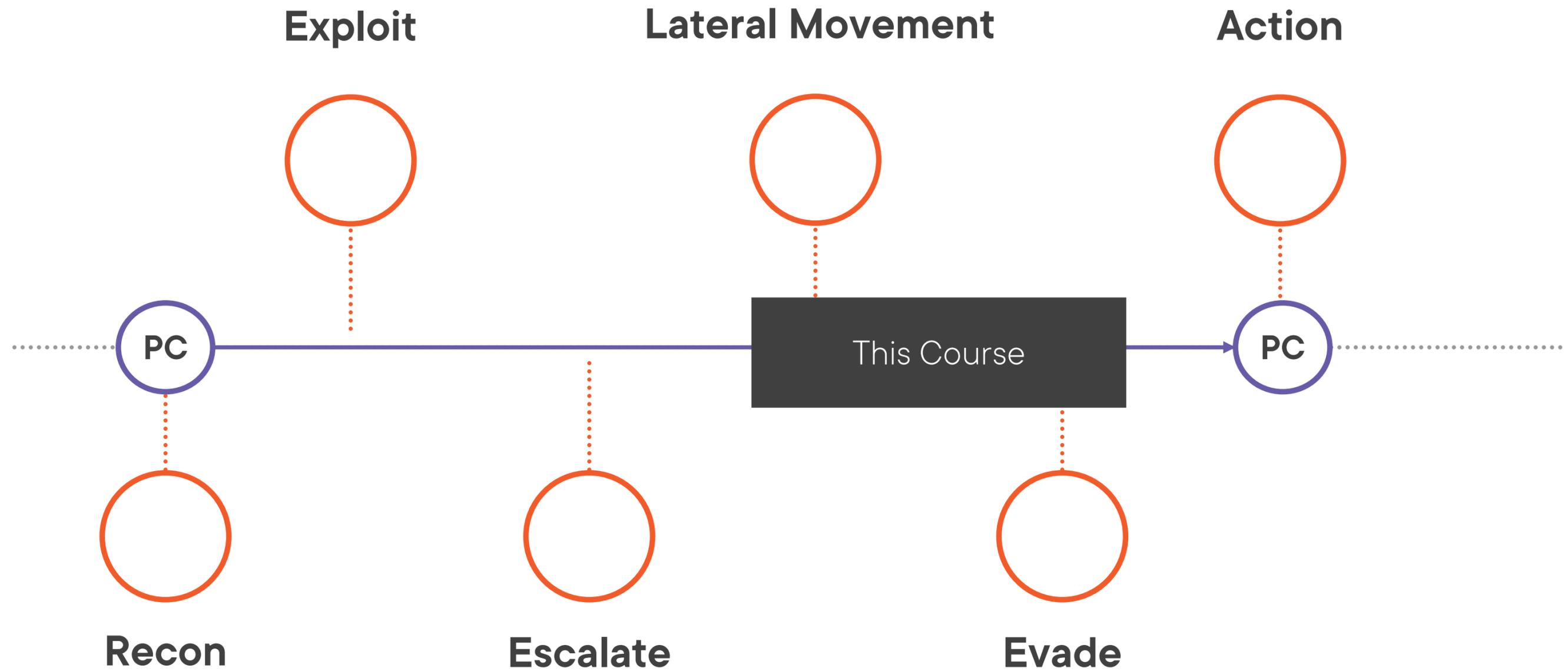
**Allows to redirect TCP packets from any tool (e.g. NMap, theHarvester, SSH, etc.)**

**Provide anonymous traffic**

**Bypass defense mechanisms**



# Kill Chain



# MITRE ATT&CK

## **Tactics**

Reconnaissance  
Resource Development  
Initial Access  
Execution  
Persistence  
Privilege Escalation  
Defense Evasion  
Credential Access  
Discovery  
Lateral Movement  
Collection  
Command & Control  
Exfiltration  
Impact



# MITRE ATT&CK

## Tactics

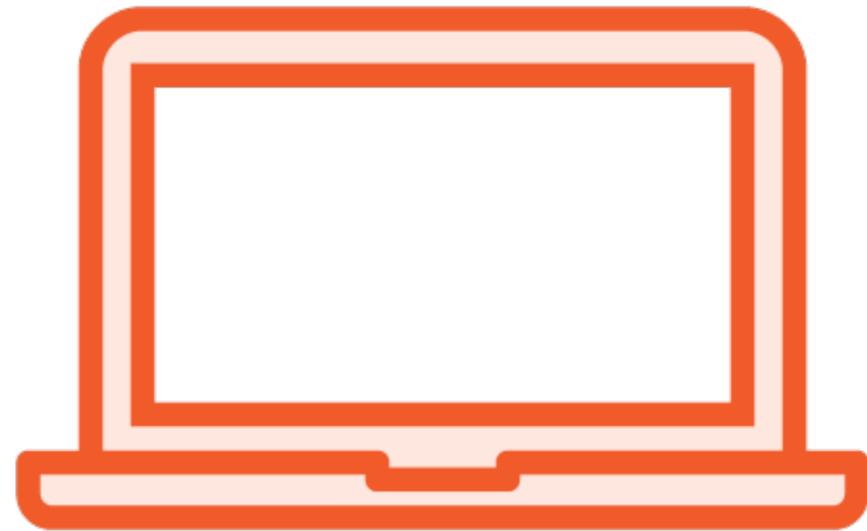
- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command & Control
- Exfiltration
- Impact

T1599:  
**Network Boundary Bridging**

⋮

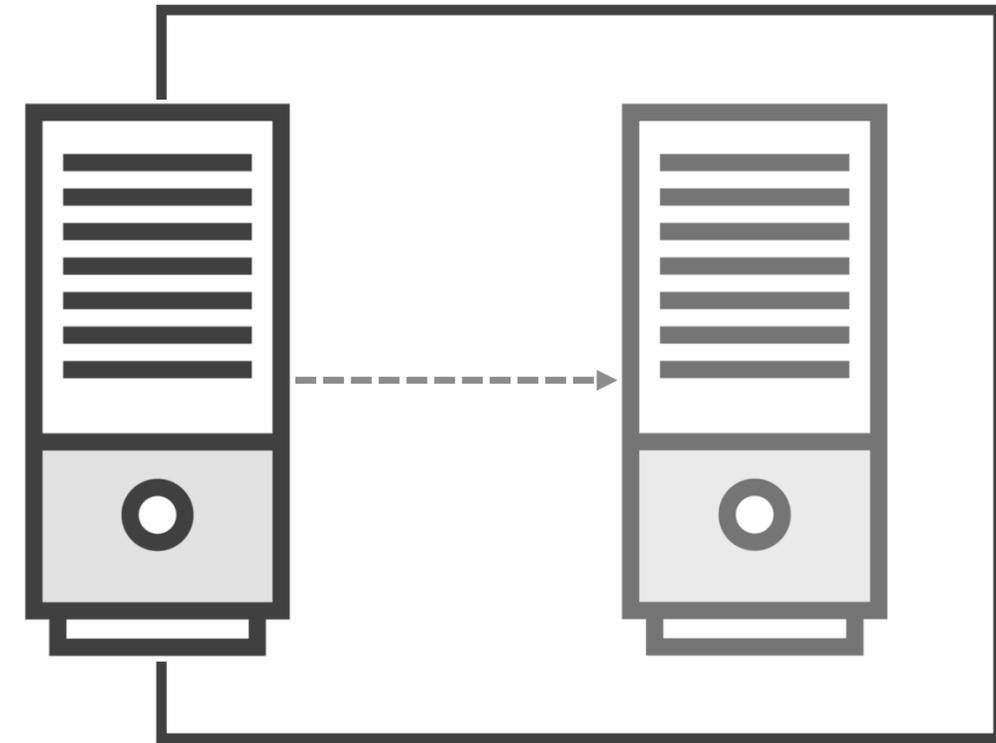


# Prerequisites



## Attacker Machine

Kali Linux or any other Linux distribution

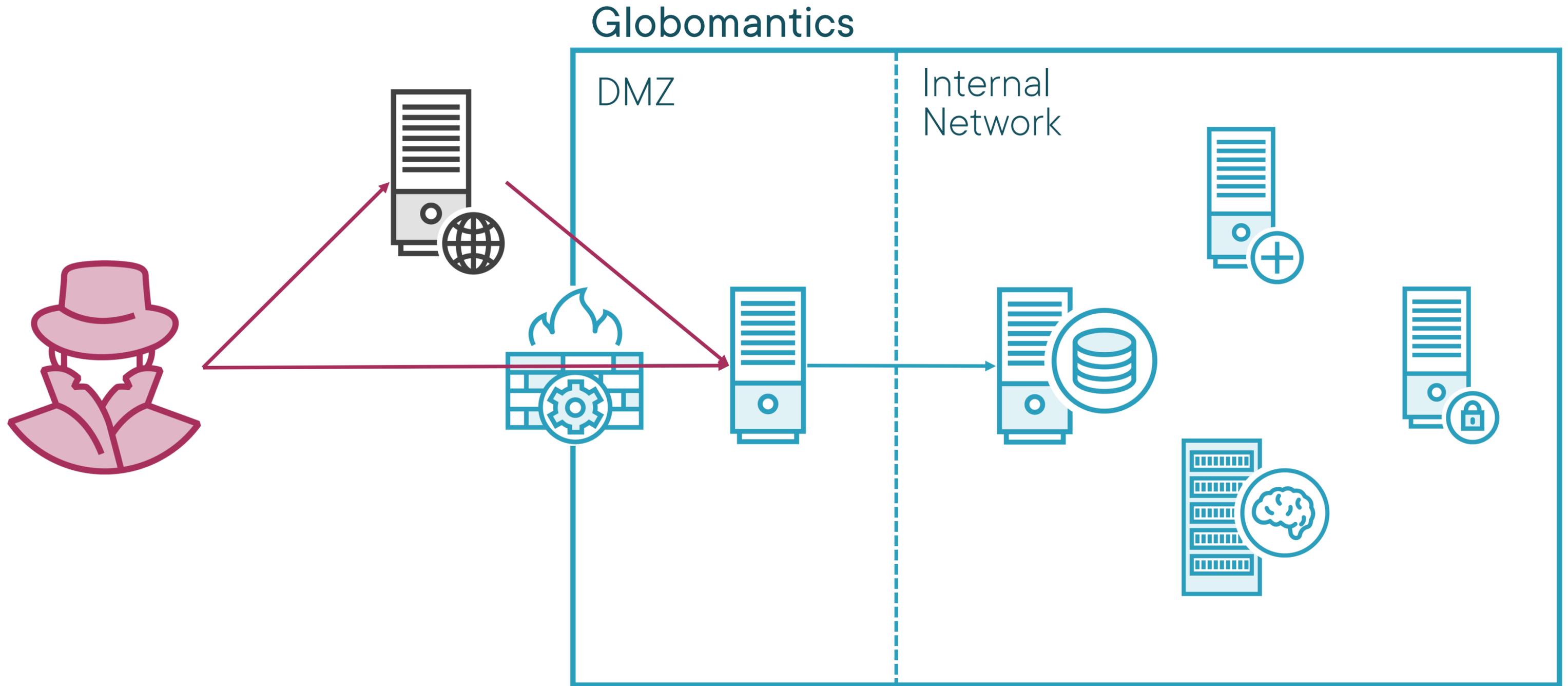


## Victim Environment

One DMZ server with access to an internal server



# Demo Part 1: Obfuscating Incoming Traffic

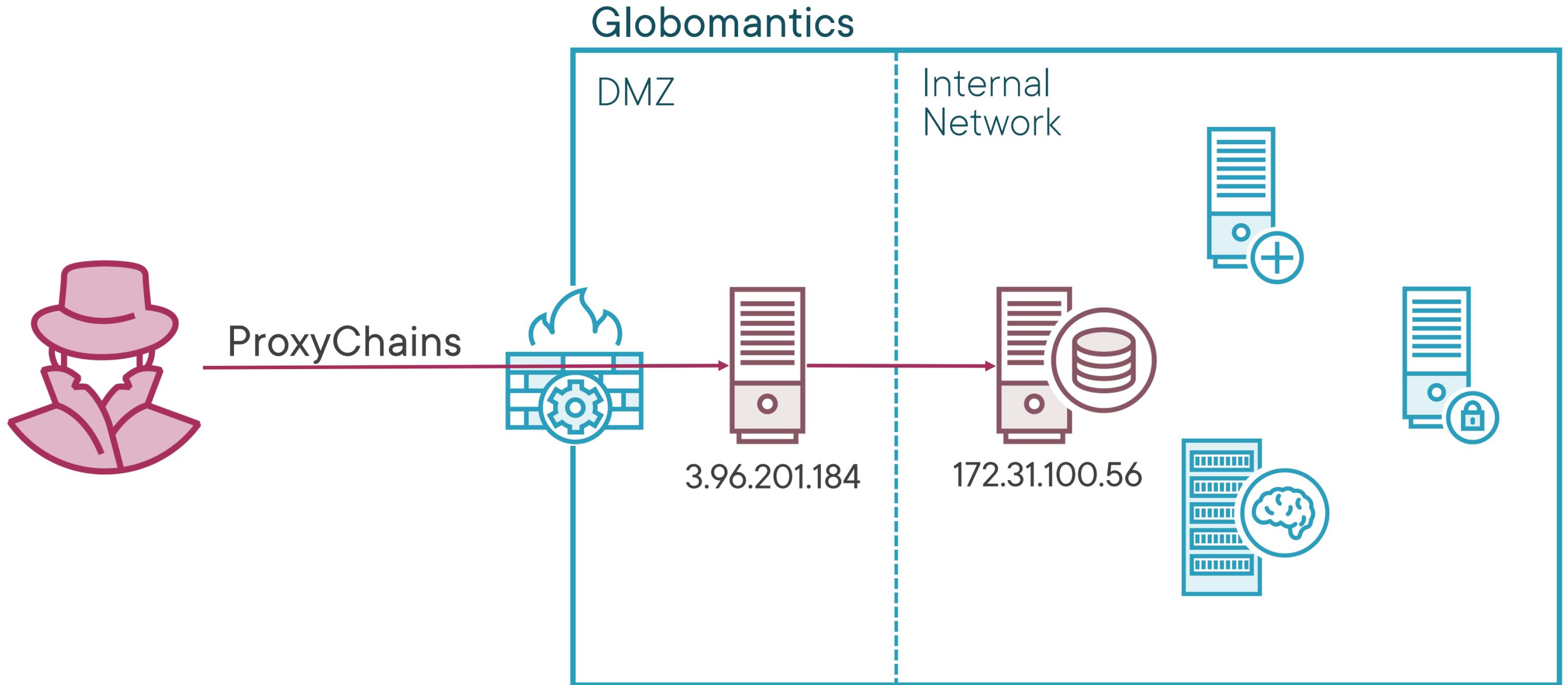


# Demo Place Holder

1. Installation Tips and Tricks
2. First use instructions and common usage syntax
3. Use of main features on live targets or in live environment



# Demo Part 2: Bypassing Network Perimeter Defense



# Demo 2 Place Holder

1. Installation Tips and Tricks
2. First use instructions and common usage syntax
3. Use of main features on live targets or in live environment



# More Information

## Official Documentation

Several other capabilities

<https://github.com/haad/proxychains>

## Other Features

Multi-proxy hopping

DNS resolution via proxy

## Other Defense Evasion Courses

“Defense Evasion with Invoke-Obfuscation”

## Remediation

Deploy network-behavior analysis tools

Proactive threat hunting



# Thank you!



**Ricardo Reimao**  
Cyber security consultant

