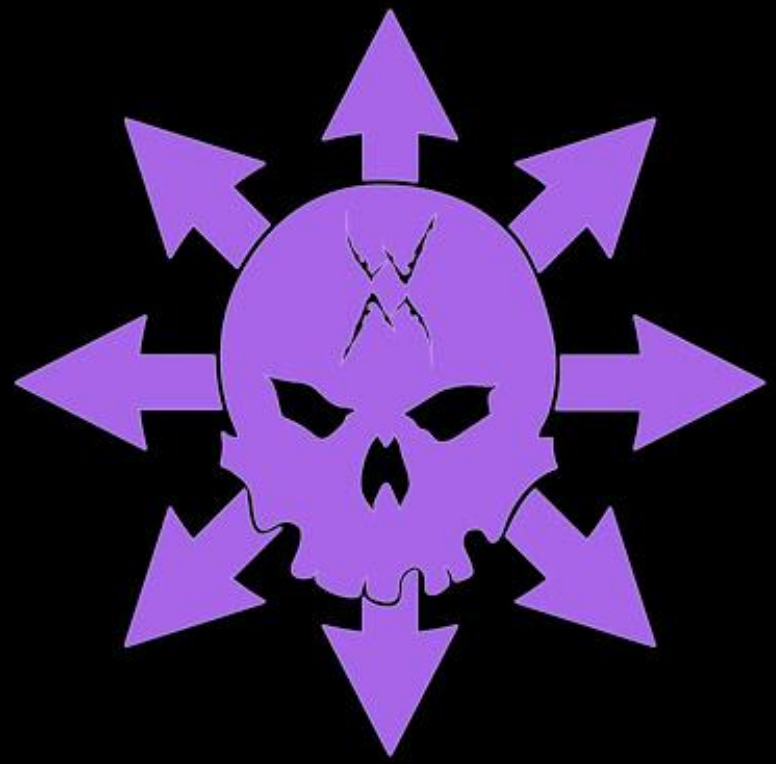
Untraceable Hacking Filtering Bypass Stealth & Chaos

GhostInTheNet
GhostInTheChaos



id $USER

Maksym Zaitsev

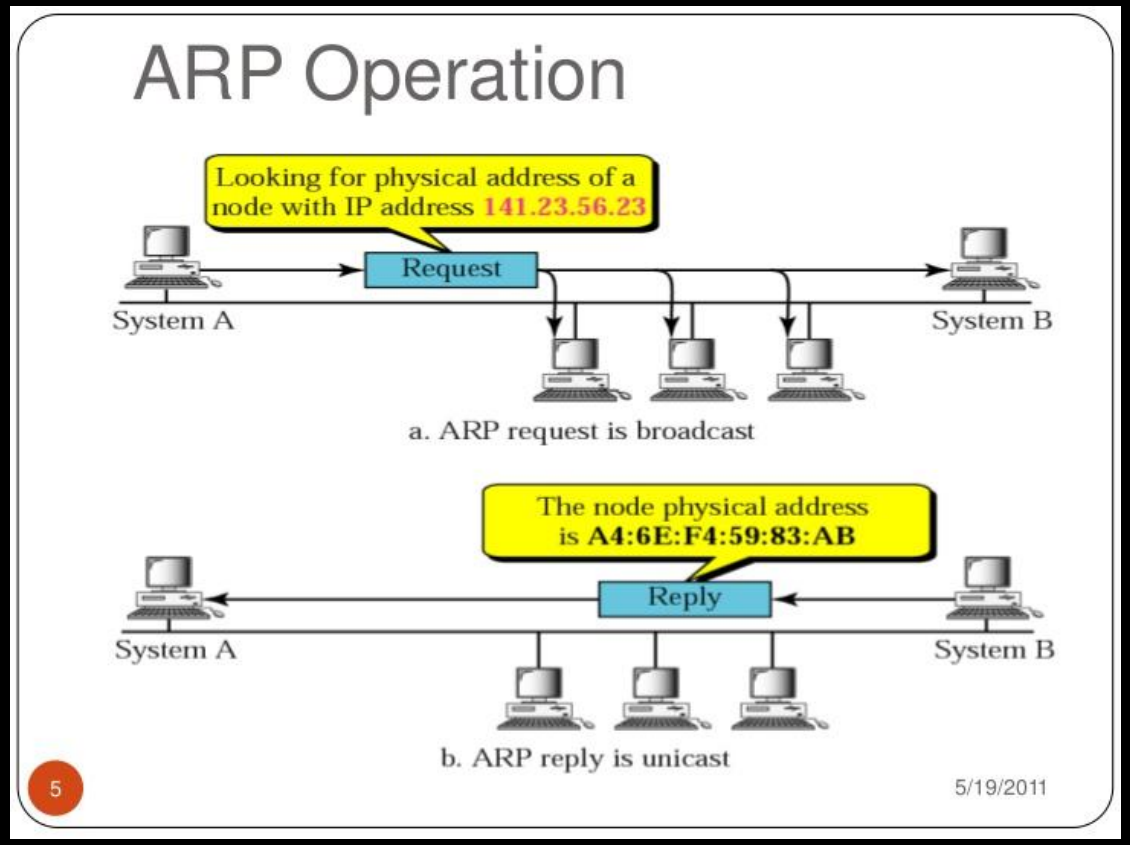
@cryptolok | Paris, France | Followers: 2.1K

github.com/cryptolok

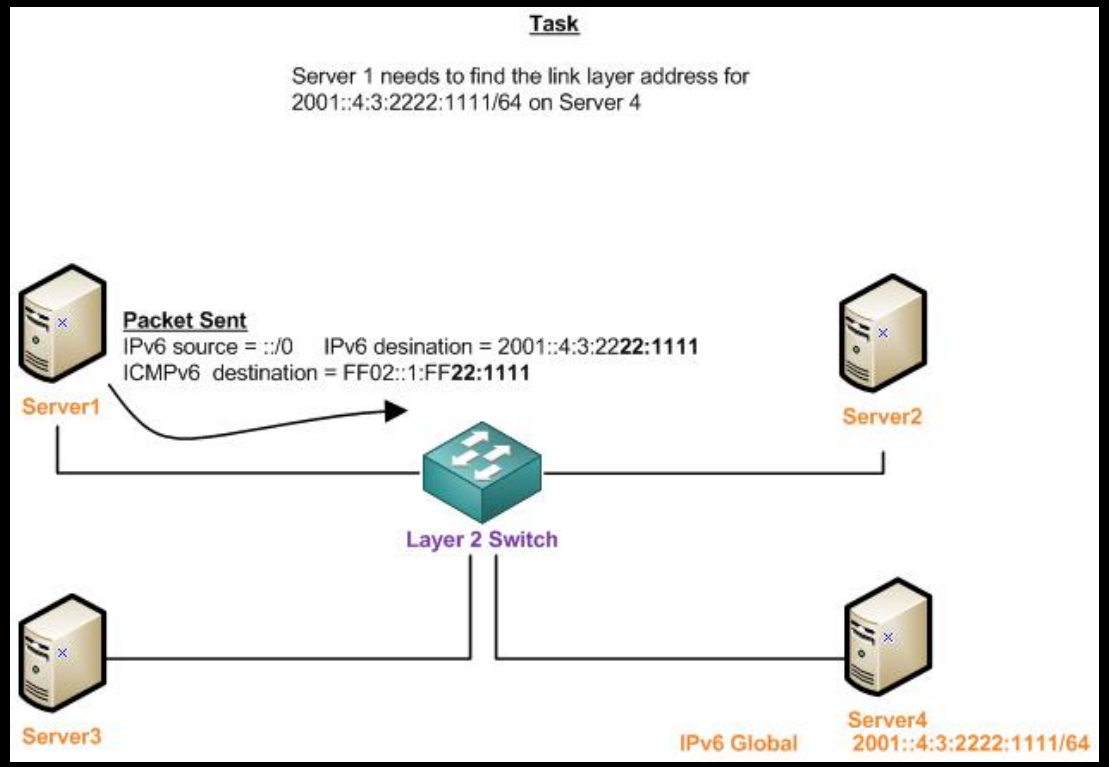
trainer, hacker, OSCP, researcher, engineer, cypherpunk : #crypto #stegano #stealth #opsec #comsec #datasec #infosec #osint #pentest #redteam #unix #hardware

@LAN

IPv4 - ARP

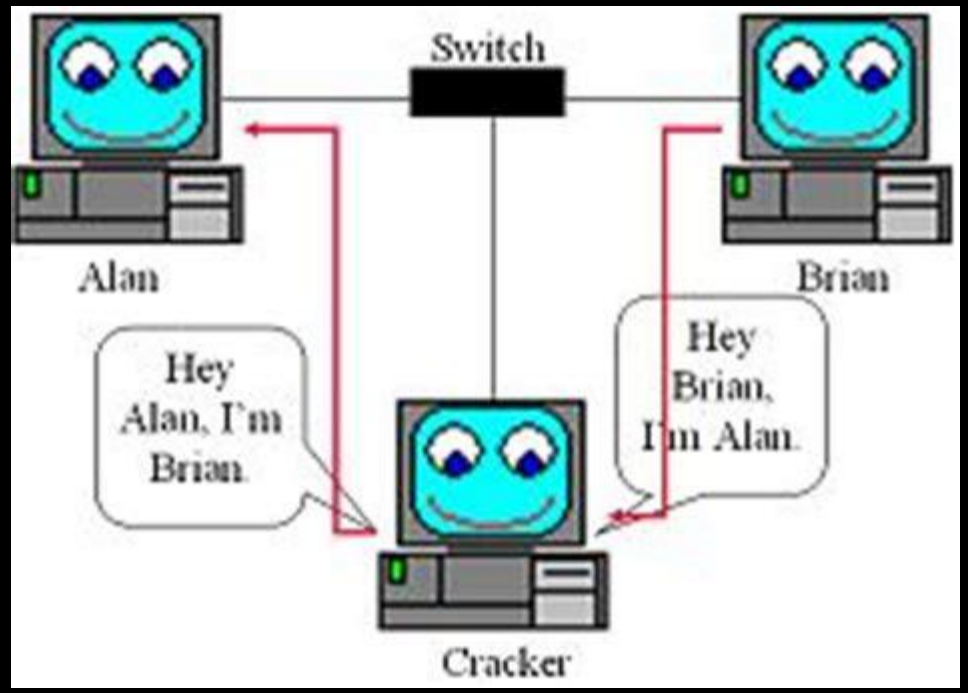


IPv6 - NDP (ICMPv6)



SECURITY/STEALTH

MITM

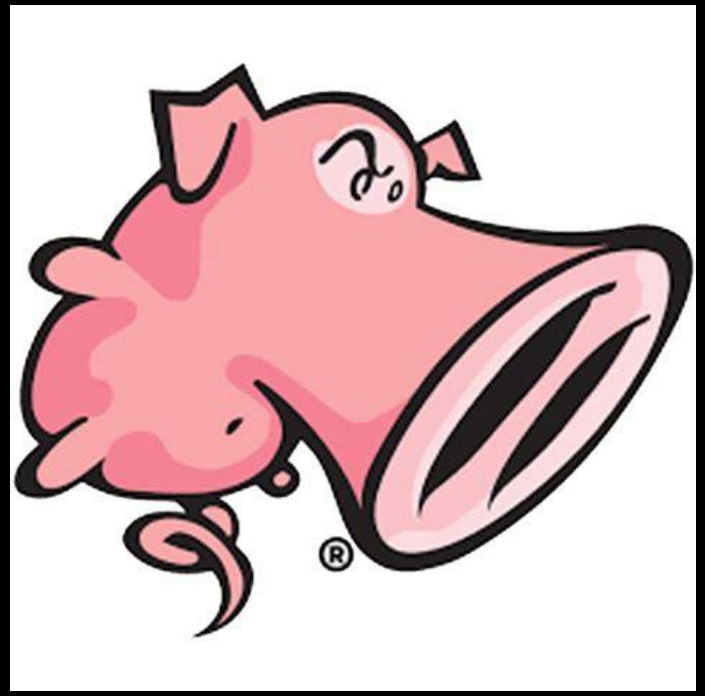


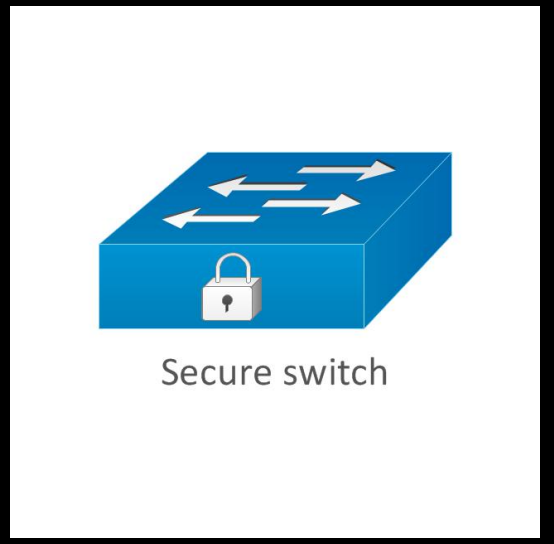
Scanning/DOS

```
Starting Nmap 6.00 ( http://nmap.org ) at 2012-05-17 12
Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.00031s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh                 2p1 Debian 3ubuntu7
| ssh-hostkey:                      :0a:d6:67:54:9d
|_2048 79:f8                        20:82:85:ec
80/tcp   o                          ((Ubuntu)
|_http-ti
9929/tcp open
Device type: gener
Running: Linux 2.6.X|3
OS CPE: cpe:/o:linux:kernel:2.6 cpe:/o:linux:kernel:3
OS details: Linux 2.6.32 - 2.6.39, Linux 2.6.38 - 3.0
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel
```

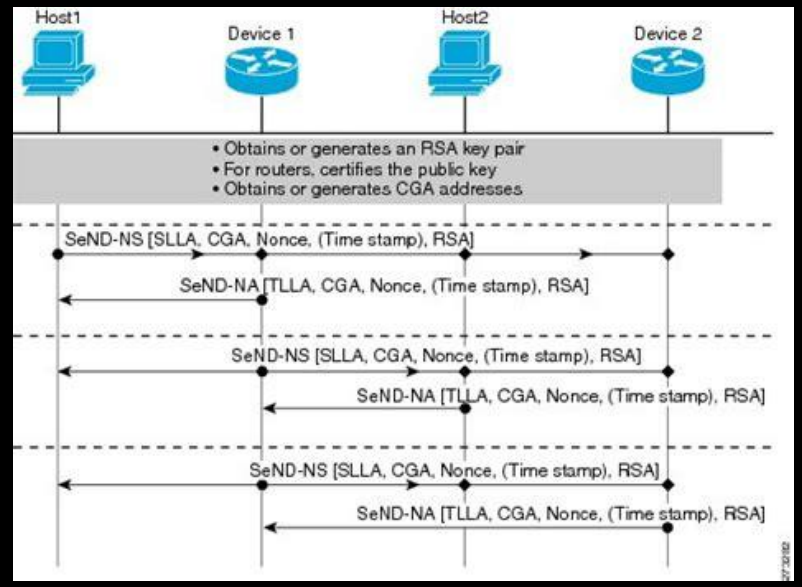
SOLUTIONS


ARPON




Secure switch


ANTI VIRUS


Host1
Device 1
Host2
Device 2
• Obtains or generates an RSA key pair
• For routers, certifies the public key
• Obtains or generates CGA addresses
SeND-NS [SLLA, CGA, Nonce, (Time stamp), RSA]
SeND-NA [TLLA, CGA, Nonce, (Time stamp), RSA]
SeND-NS [SLLA, CGA, Nonce, (Time stamp), RSA]
SeND-NA [TLLA, CGA, Nonce, (Time stamp), RSA]
SeND-NS [SLLA, CGA, Nonce, (Time stamp), RSA]
SeND-NA [TLLA, CGA, Nonce, (Time stamp), RSA]

IDEA

Network Invisibility

Network Anonymity

Protection from MITM/DOS

Cross-Platform

Ressource-Efficent

Minimalistic

GhostInTheNet

Spoof MAC => IP

Spoof Hostname => DHCP

Ignore ARP broadcast

Restrict ARP to unicast

Ignore ICMPv6/NDP echo/soliciation

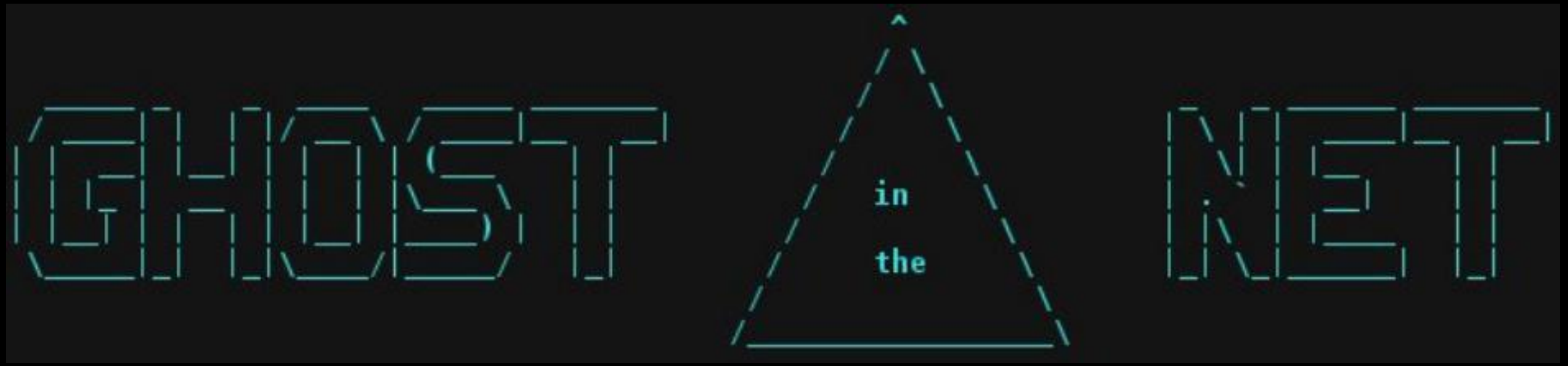
IPtables
SHELL

offsec

pentest

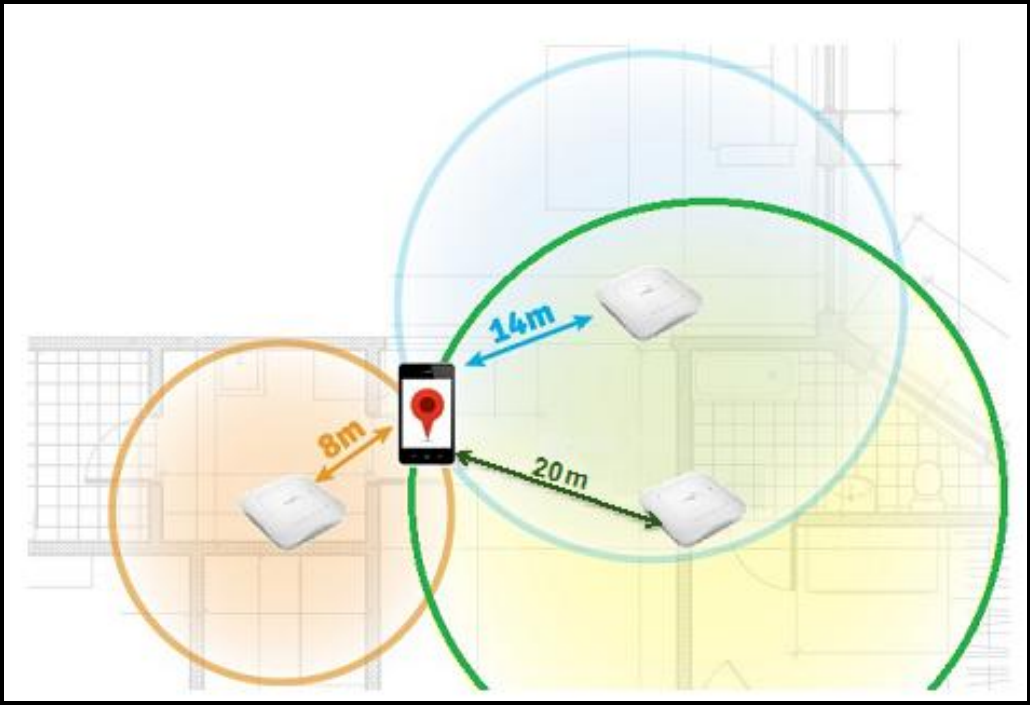
redteam

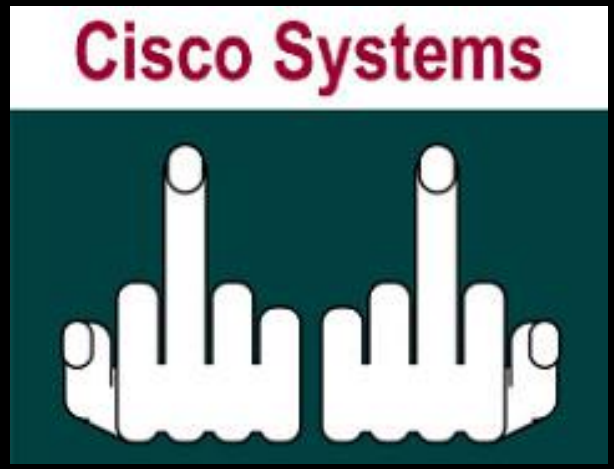
DEMO

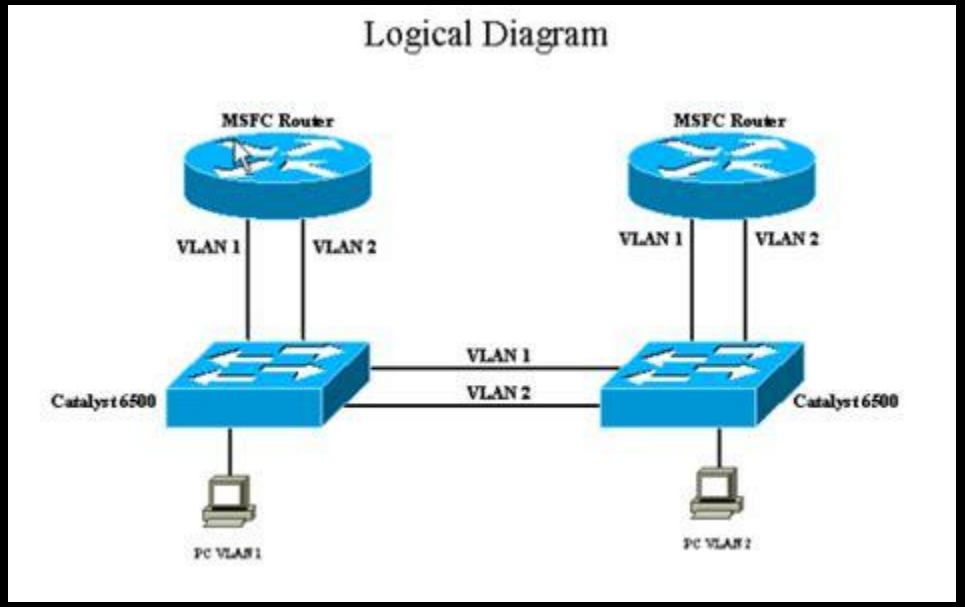


LIMITATIONS/MITIGATIONS

Dynamic ARP Inspection
sticky MAC







@WAN

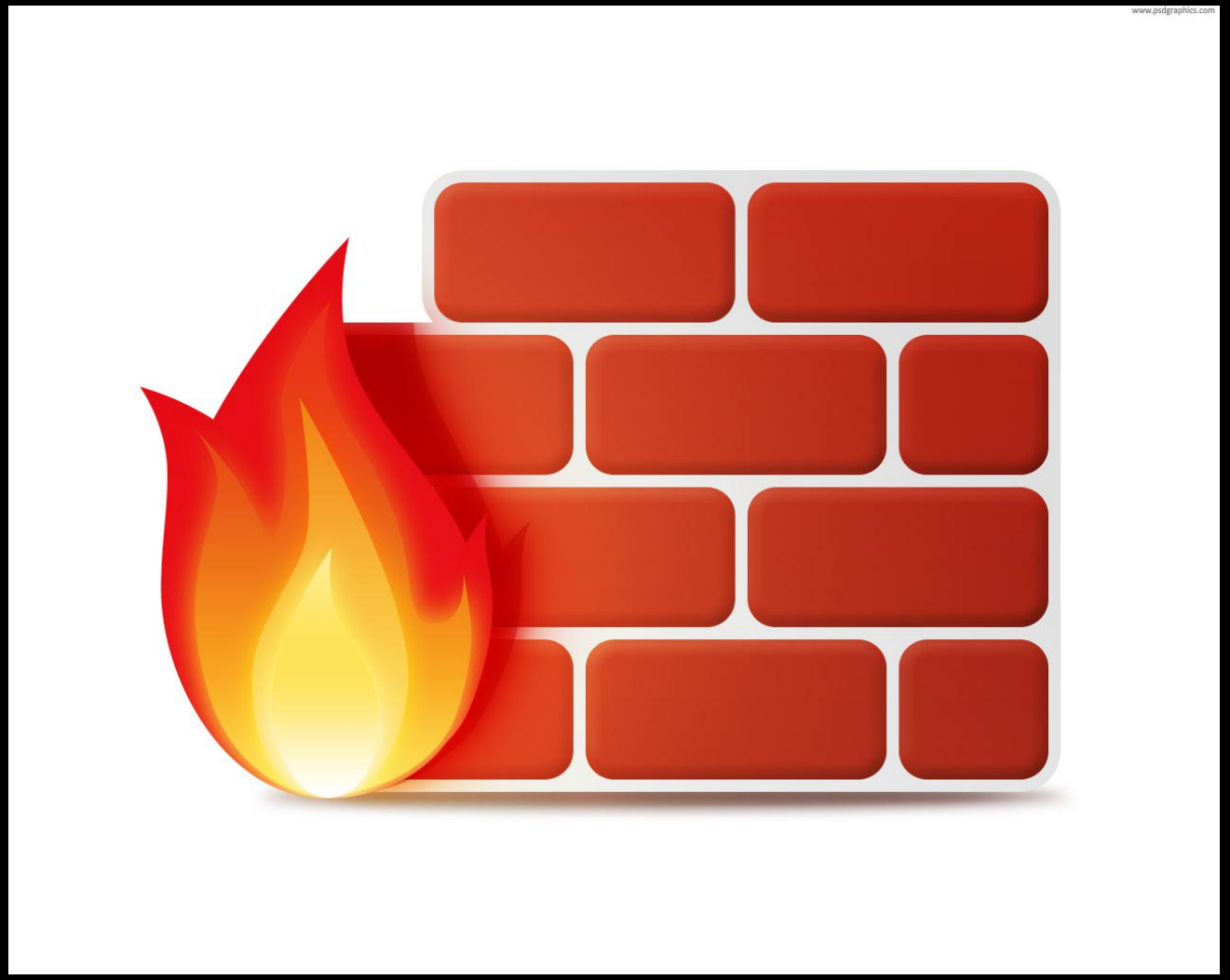
SECURITY/STEALTH

Corporate WAF/firewall

ISP/DPI monitoring

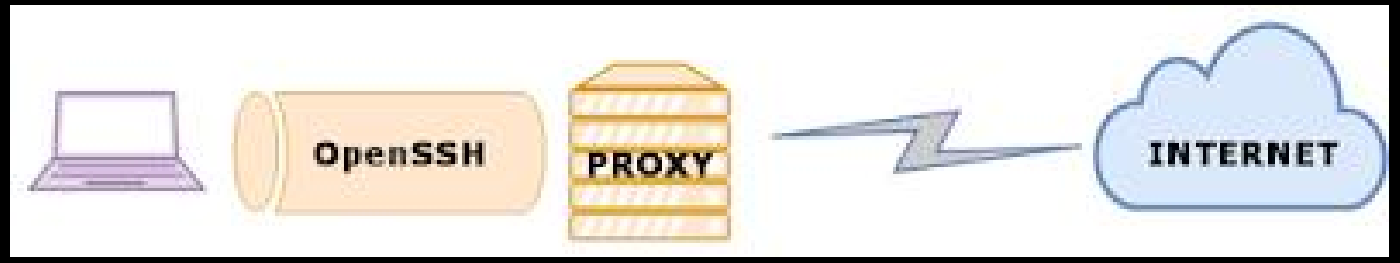
Censorship

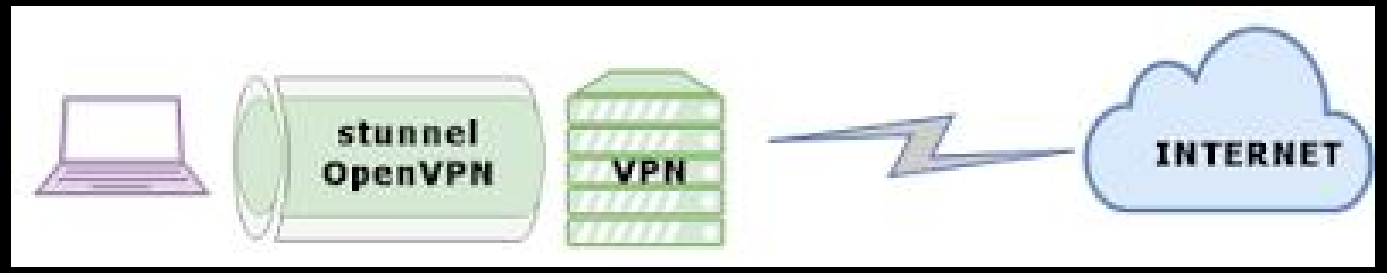
Tracing



SOLUTIONS

DNSCrypt (IP) Proxy (sec) PortForwaring (limited)
VPN (DPI/logs) Tor (bridges)





IDEA

Client protection

Server invisibility

Bypass censorship

Bypass network filtering

Transparent

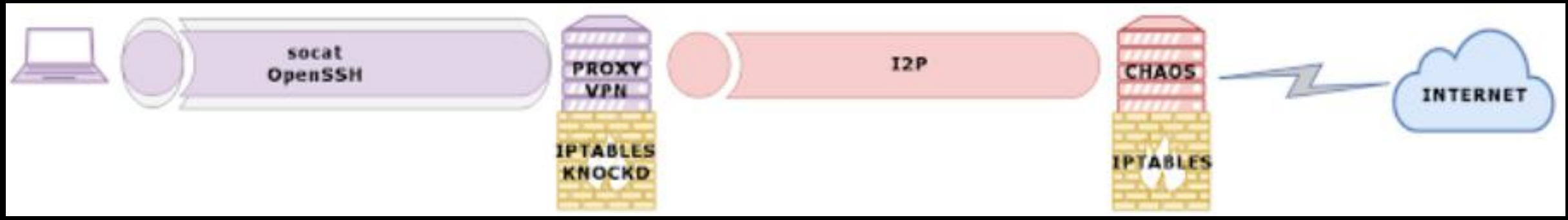
Cross-Platform

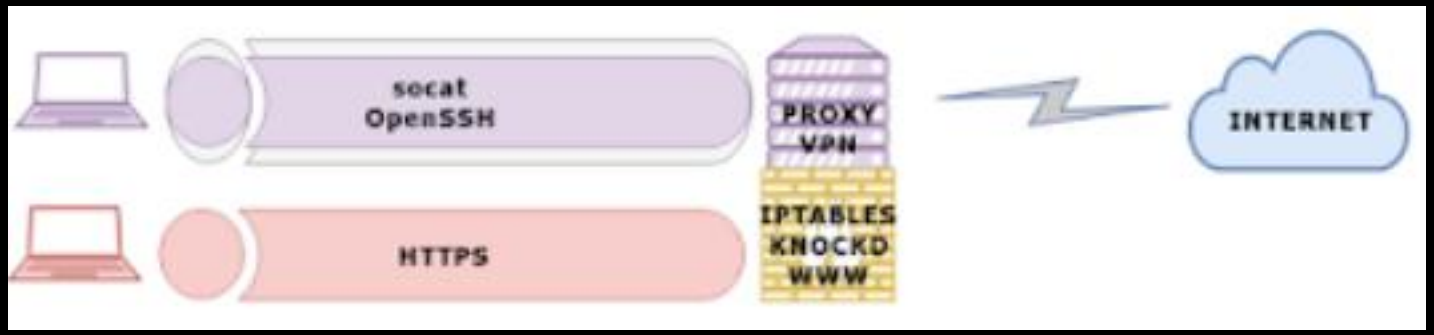
Minimalistic

GhostInTheChaos

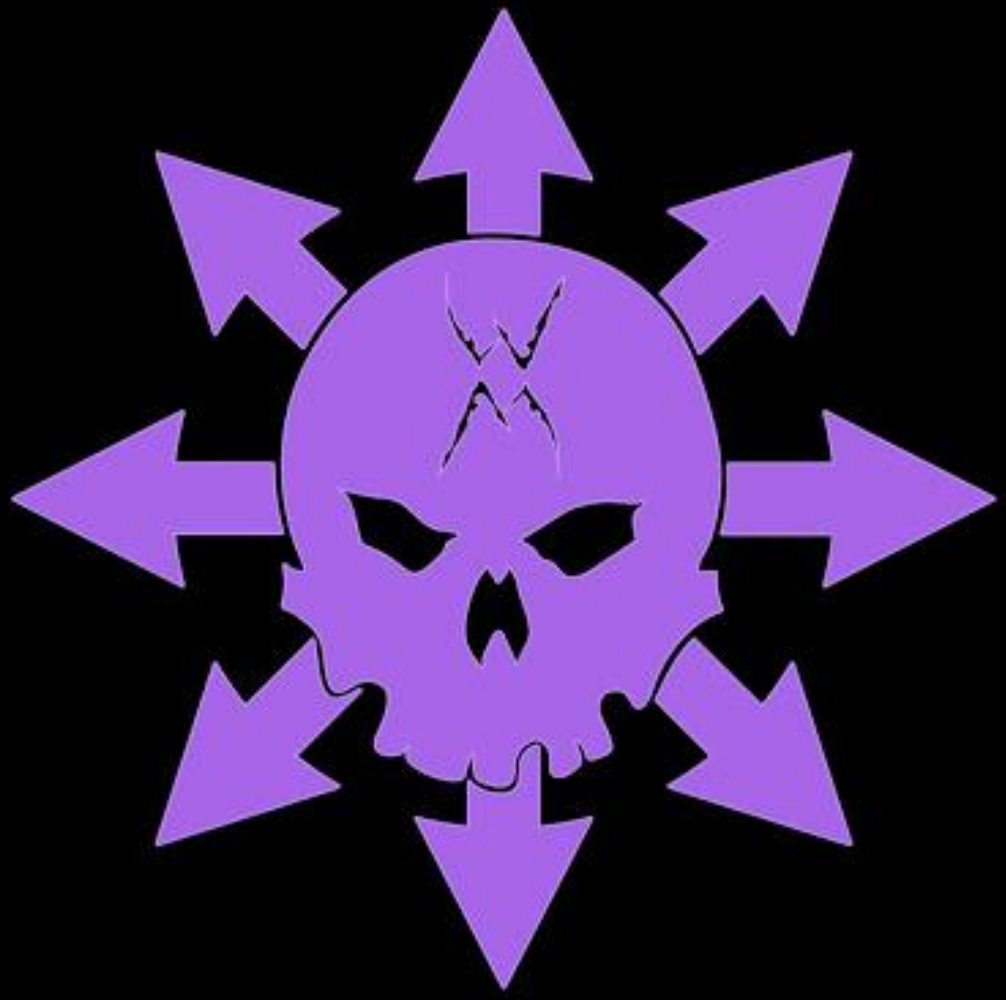
Block server input & SSL encapsulation
SSH tunnel & chaotic routing
Android

SHELL OpenSSH
IPtables kncokd
socat I2P





DEMO



LIMITATIONS

Reduced speed for anonymity (abuse prevention)

Domain names are preferable (cost)

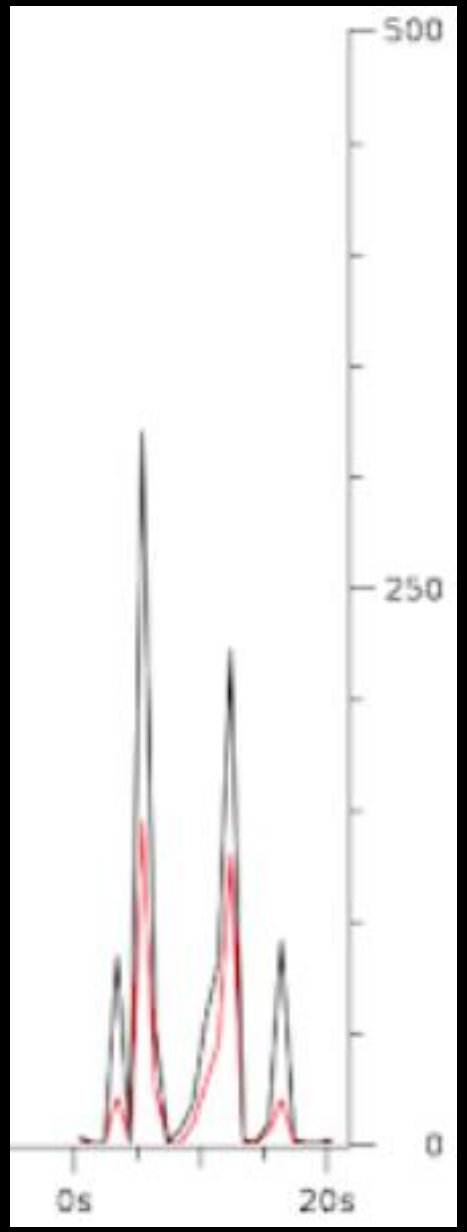
Scanning "obscurity" (hardening)

Android limited support

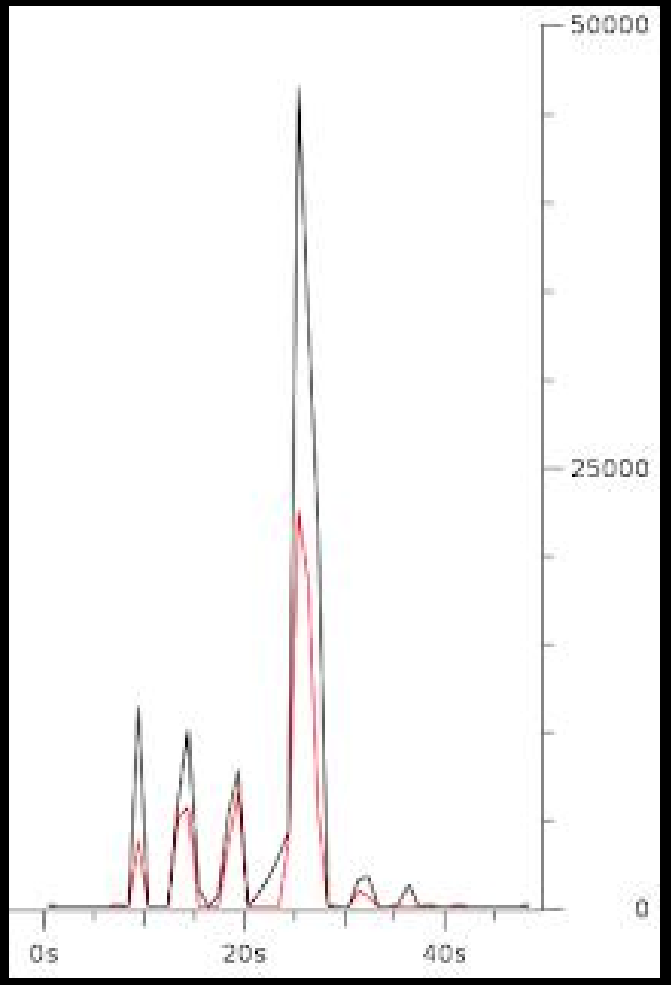
MITM certificate

MITIGATIONS

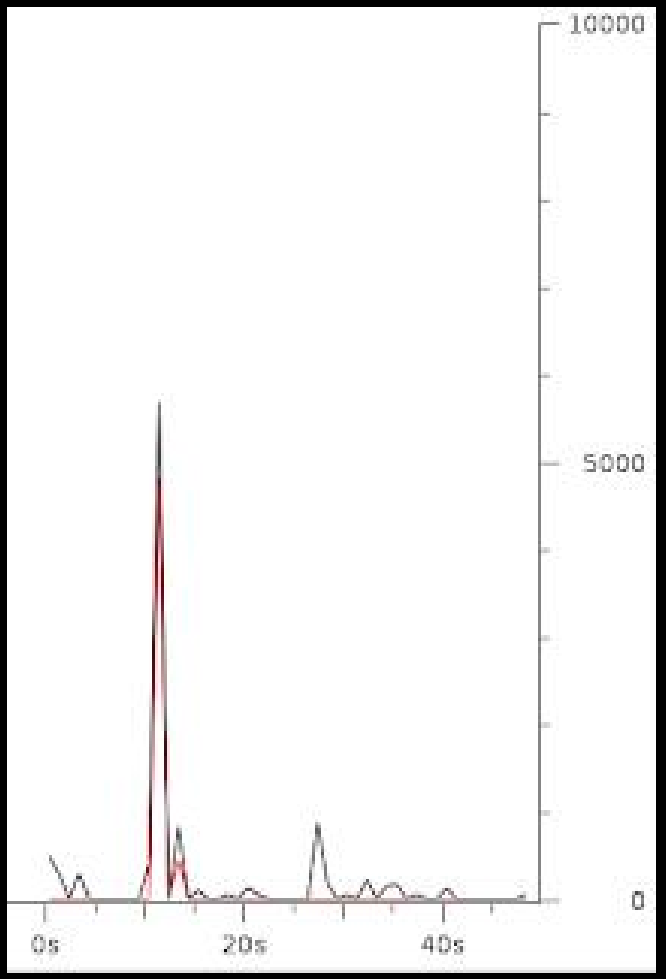
HTTPS



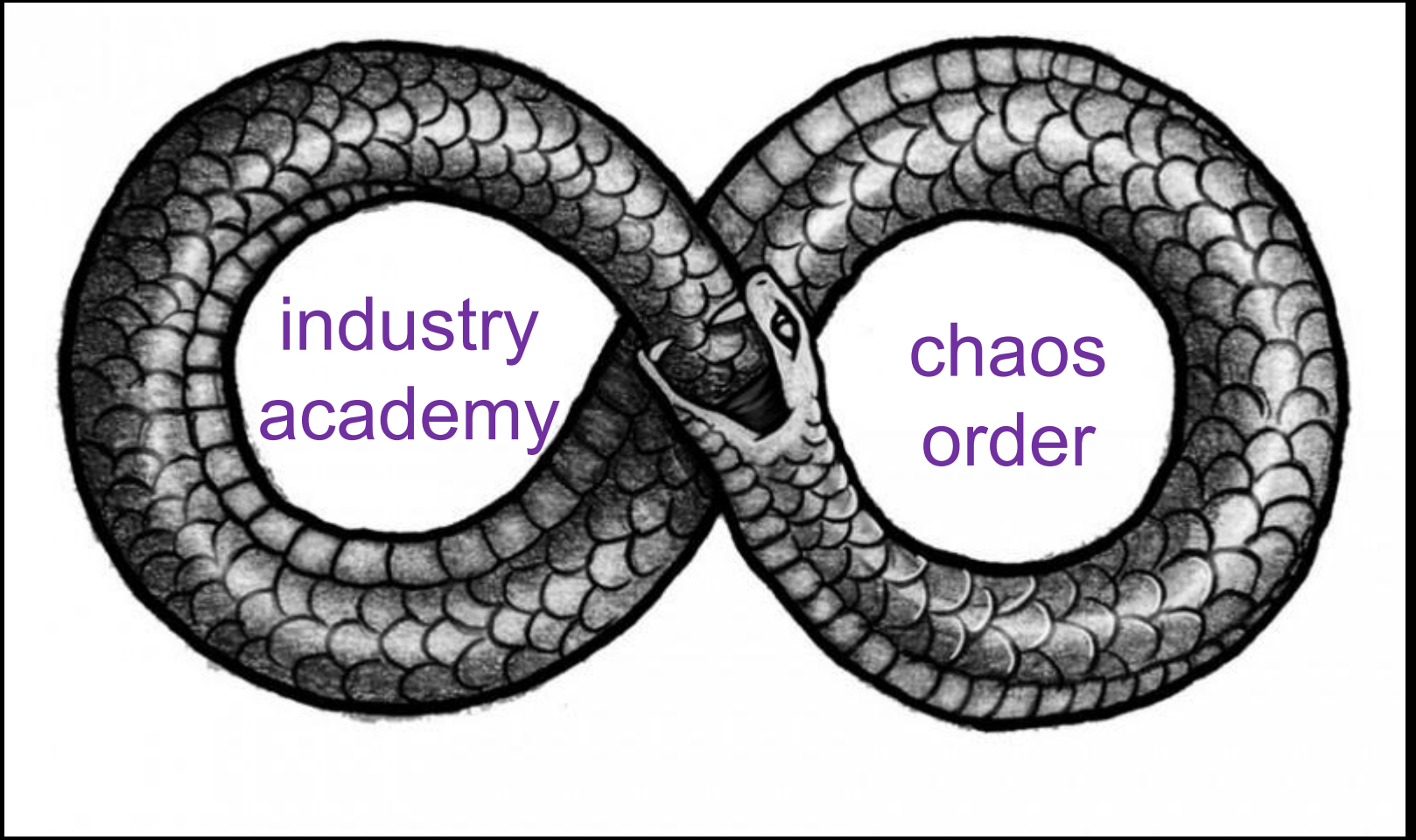
SSH+socat



VPN+socat



CONCLUSION



QUESTIONS/NOTES?

Maksym Zaitsev
@cryptolok