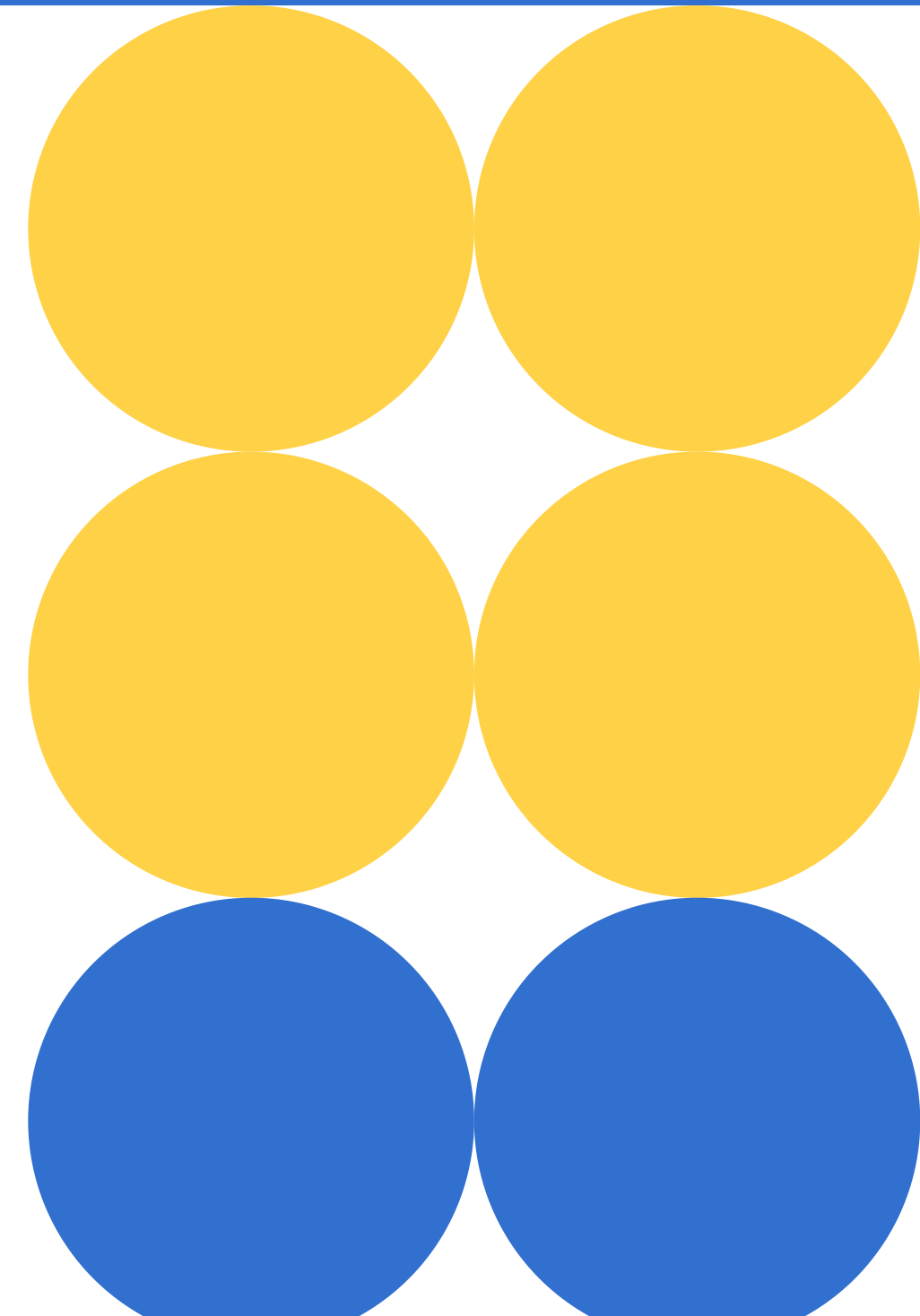




Armillotta Michele +
De Divitiis Edoardo
Raffaelli Andrea

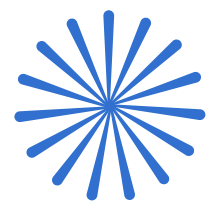
DDoS mitigation and anti-scan filtering with eBPF and XDP



Introduzione

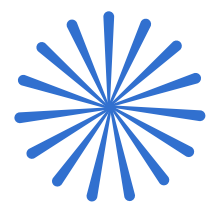
- + **Crescenti Attacchi** Con il crescente numero di attacchi c'è la necessità di controllare il traffico proveniente dall'esterno
- + **Obiettivo** Mitigazione degli attacchi (D)DoS e di pratiche enumerative come il port scanning
- + **Nuova tecnologia** Utilizzo di una nuova tecnologia che permette più flessibilità ed efficienza rispetto i tradizionali tool del kernel Linux





Riduzione dell'overhead

XDP filtra i pacchetti prima che raggiungano lo stack di rete del kernel.



Flessibilità

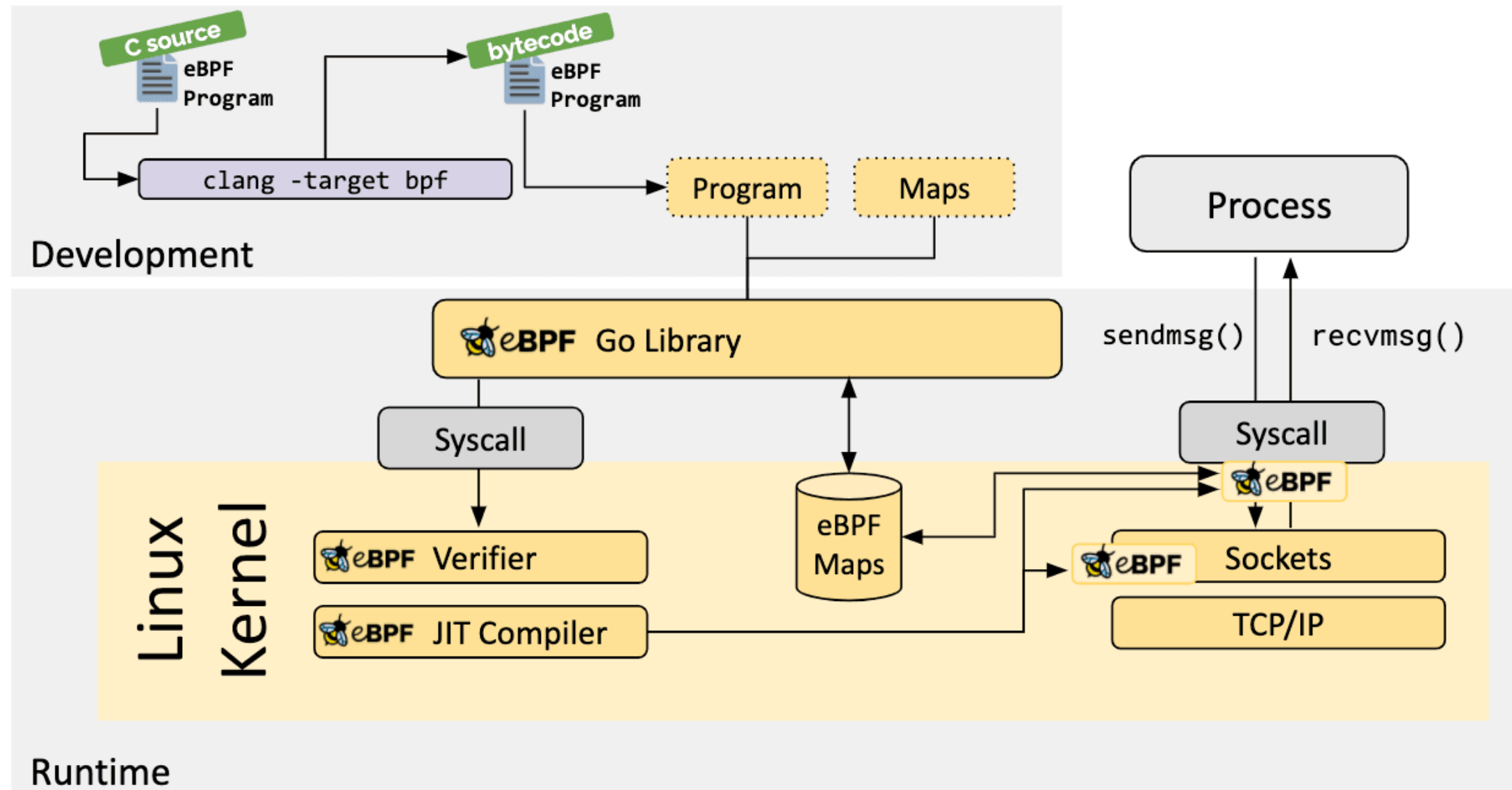
Rispetto a strumenti come DPDK, XDP offre un buon equilibrio tra prestazioni e supporto nativo nel kernel Linux.



Motivazioni



eBPF



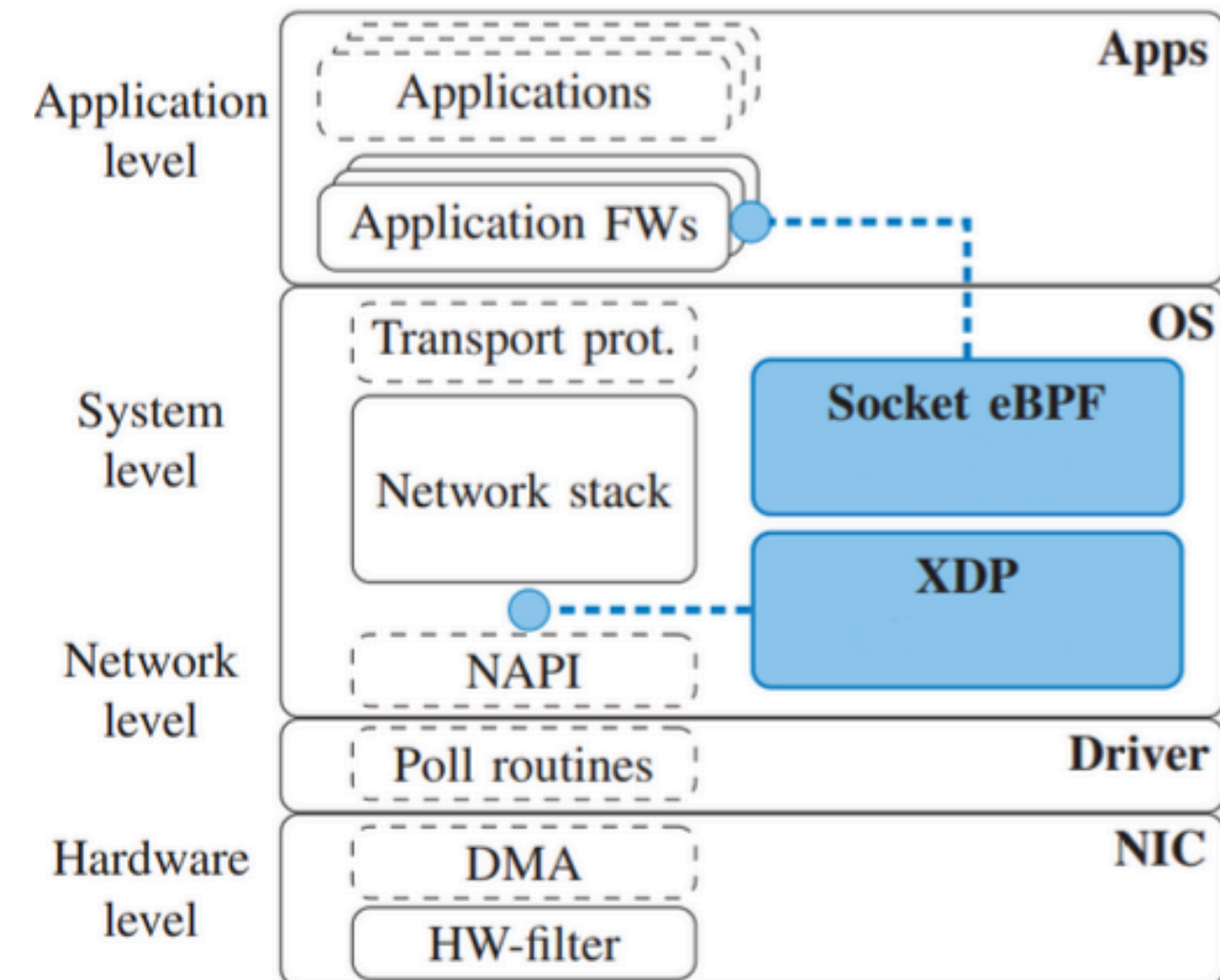
Extended Berkeley Packet Filter:

- + Esegue codice personalizzato nel kernel in modo sicuro ed efficiente
- + I programmi sono event driven e vengono attaccacati a degli hook point
- + Usato in una grande varietà di modi: dal networking ad alte prestazioni al load-balancing nei data centers

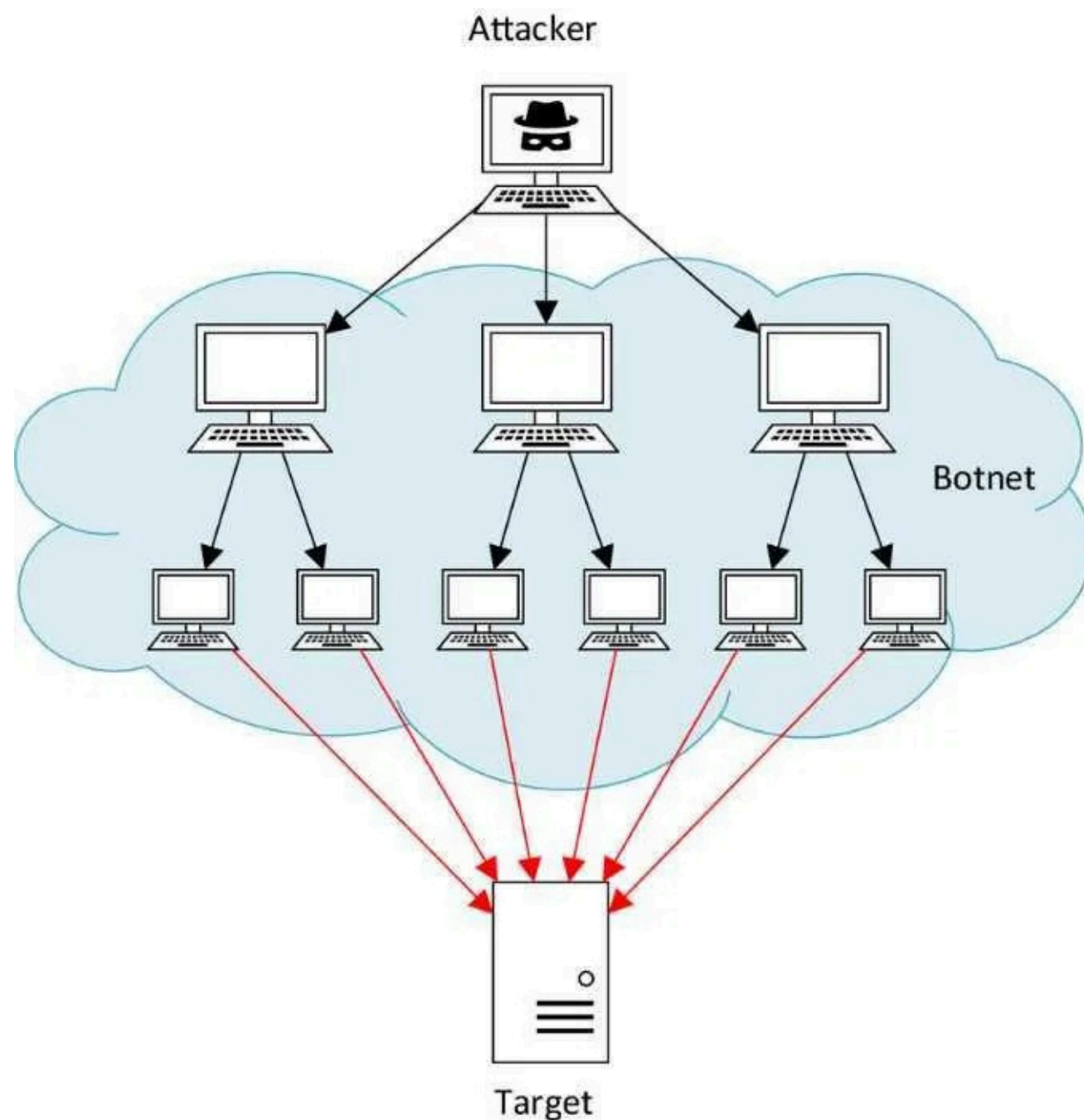
XDP

eXpress Data Path:

- + Processa i pacchetti con alte prestazioni direttamente nel driver di rete.
- + Benefici principali: Bassa latenza, riduzione del carico CPU, filtraggio tempestivo dei pacchetti.



(D)DoS e Port Scanning



+ Distributed Denial of Service:

Tipo di attacco informatico che mira a rendere un servizio, un sito web o una risorsa di rete inaccessibile agli utenti legittimi, sovraccaricando il sistema target

Le conseguenze di un attacco DDoS possono includere:

- Perdite finanziarie per aziende e organizzazioni
- Danni alla reputazione
- Costi legati alle attività di recupero e mitigazione

+ Port scanning

Tecnica utilizzata per identificare le porte aperte su un sistema di rete: rappresentano punti di accesso per la comunicazione tra dispositivi e applicazioni

+ **Ambiente di sviluppo e test**

VM con Debian 11 e driver di rete e1000.

Provisioning avanzato con Vagrant.

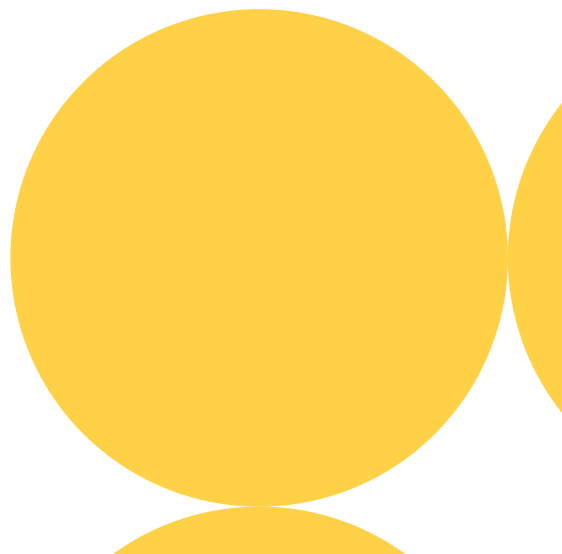
+ **Modalità XDP-generic**

Esecuzione emulata di programmi XDP

+ **Building framework**

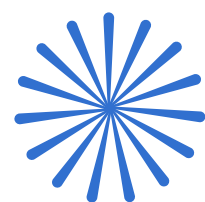
libbpf-bootstrap per facilitare l'utilizzo di eBPF.

Architettura del sistema - Setup



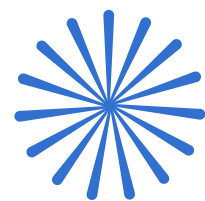
DoS detector - Architettura

L'architettura è costituita da due componenti:



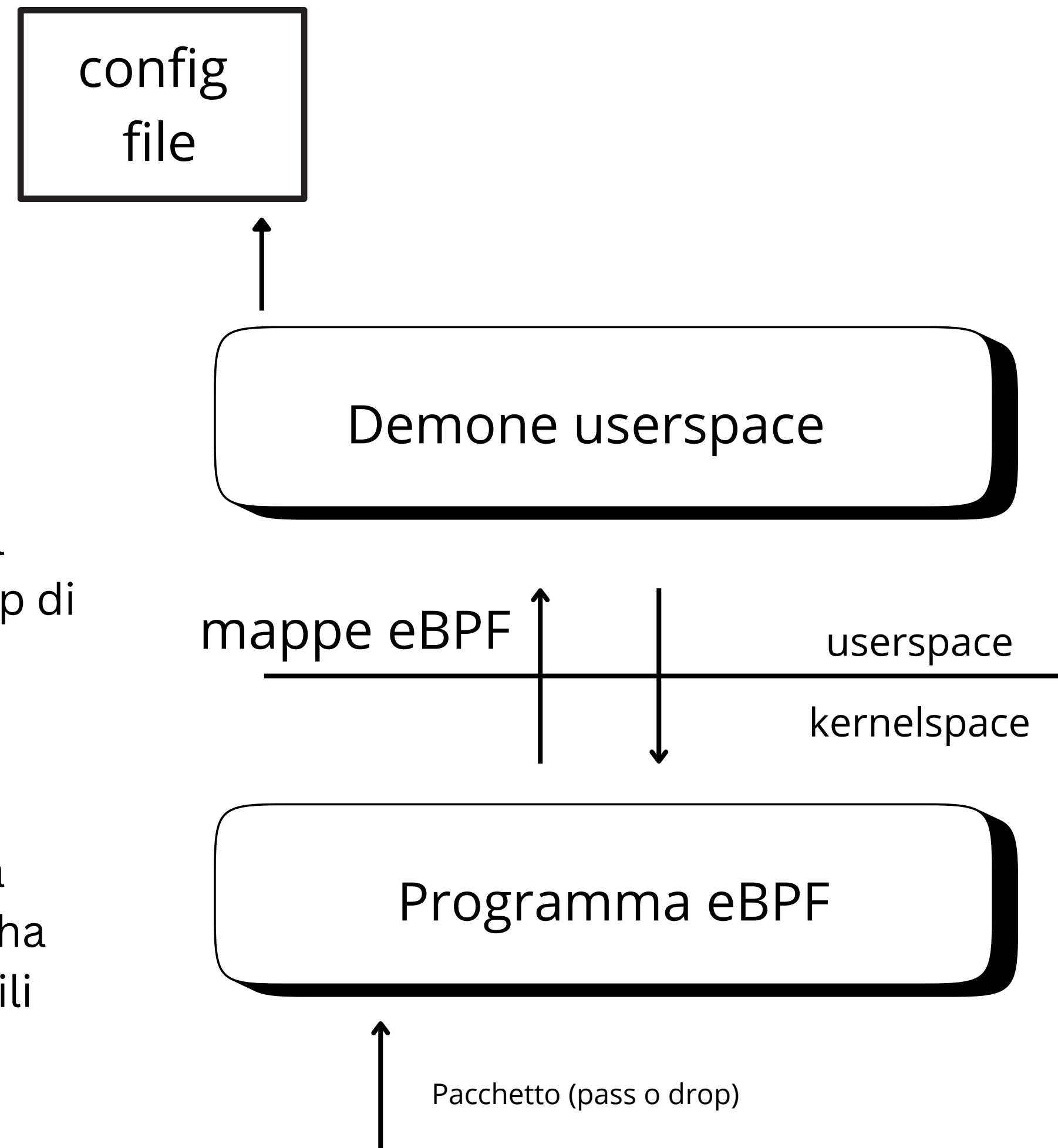
Demone userspace

Legge la configurazione dell'utente, carica il programma eBPF nel kernel e gestisce il loop di aggiornamento dell'orologio logico



Programma eBPF

Viene attivato per ogni pacchetto che arriva all'hook XDP e controlla se uno specifico ip ha superato la threshold di pacchetti trasmissibili per secondo, nel caso lo scarta.



Test e Risultati – (D)DoS Detector

Interval	Transfer	Bitrate
3.00-4.00 sec	11.9 MBytes	100 Mbits/sec
4.00-5.00 sec	11.9 MBytes	100 Mbits/sec
5.00-6.00 sec	3.35 MBytes	28.0 Mbits/sec
6.00-7.00 sec	1.10 MBytes	9.21 Mbits/sec

Nel momento in cui l'attacco viene effettuato vediamo la banda che cala drasticamente



Test funzionali:

1 server UDP attaccato da hping
1 server iperf3 per monitorare la qualità del servizio e lo stress della macchina



Risultati:

Successo nel blocco IP
Limiti di performance: Modalità XDP-generic riduce le prestazioni.
Performance: ~250,000 pps (molto inferiore al potenziale massimo).

Anti scan - Architettura

L'architettura è costituita da due componenti:



Demone userspace

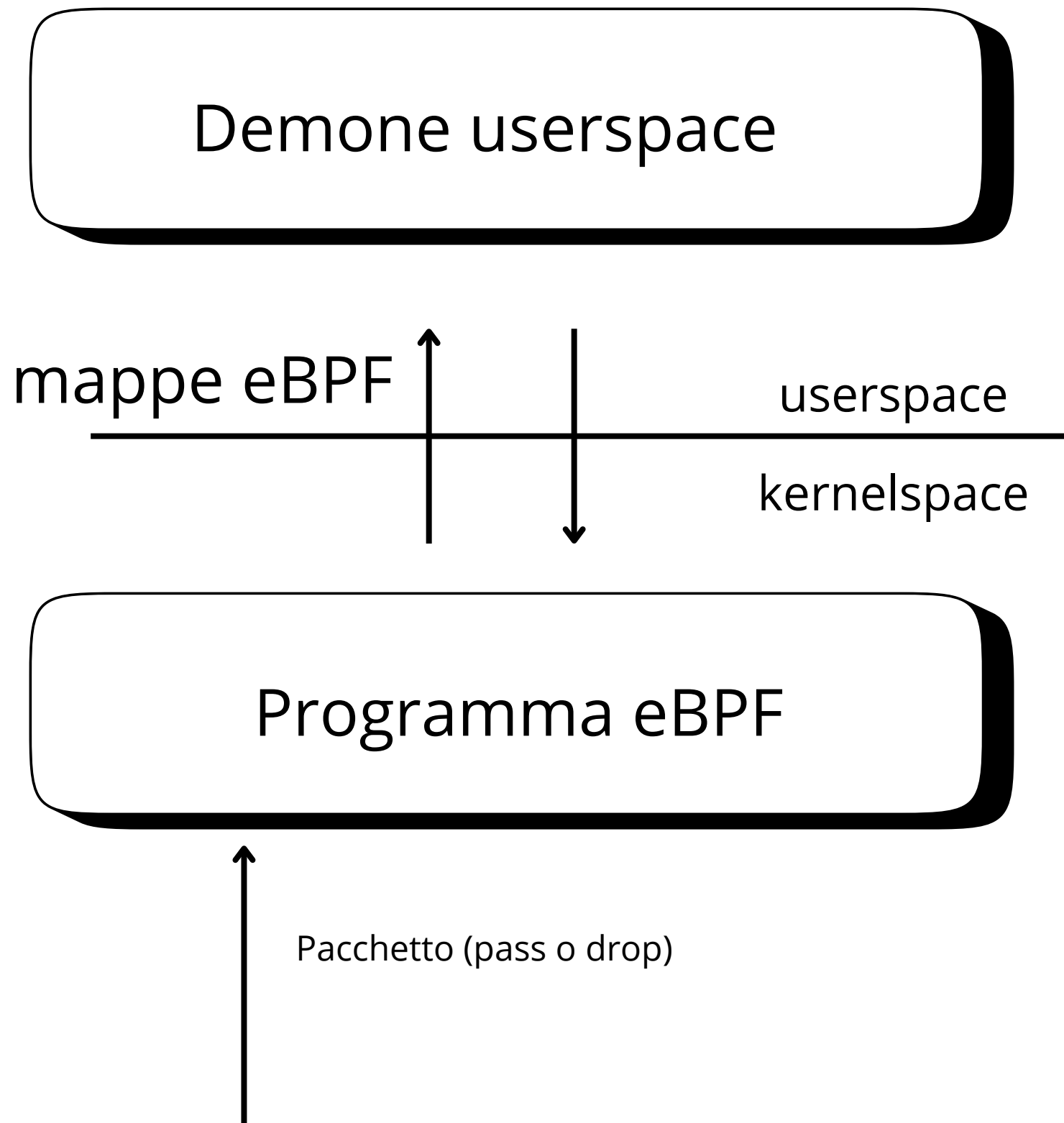
Carica il programma eBPF nel kernel, gestisce la comunicazione e aggiorna la blacklist



Programma eBPF

Implementato con XDP, analizza i pacchetti in arrivo, verifica la legittimità di una connessione e blocca i tentativi di scansione

La sincronizzazione avviene tramite eBPF maps e un orologio logico.



Test e Risultati – Anti scan

Name	Interval	Transfer	Bitrate
Host (sender)	0.00-10.00 sec	4.14 GBytes	3.55 Gbits/sec
VM without BPF (receiver)	0.00-10.00 sec	4.14 GBytes	3.55 Gbits/sec

Banda con programma eBPF disattivato

Name	Interval	Transfer	Bitrate
Host (sender)	0.00-10.00 sec	1.20 GBytes	1.03 Gbits/sec
VM with BPF (receiver)	0.00-10.00 sec	1.19 GBytes	1.02 Gbits/sec

Banda con programma eBPF attivo



Test funzionali:

Viene effettuata l'enumerazione delle porte con nmap. le performance vengono misurate con iperf3



Risultati:

Vediamo un'ottima protezione dal tool di enumerazione, ma l'hoverhead introdotto dalla soluzione è significativo. XDP-generic riduce le prestazioni

Conclusioni e sviluppi futuri



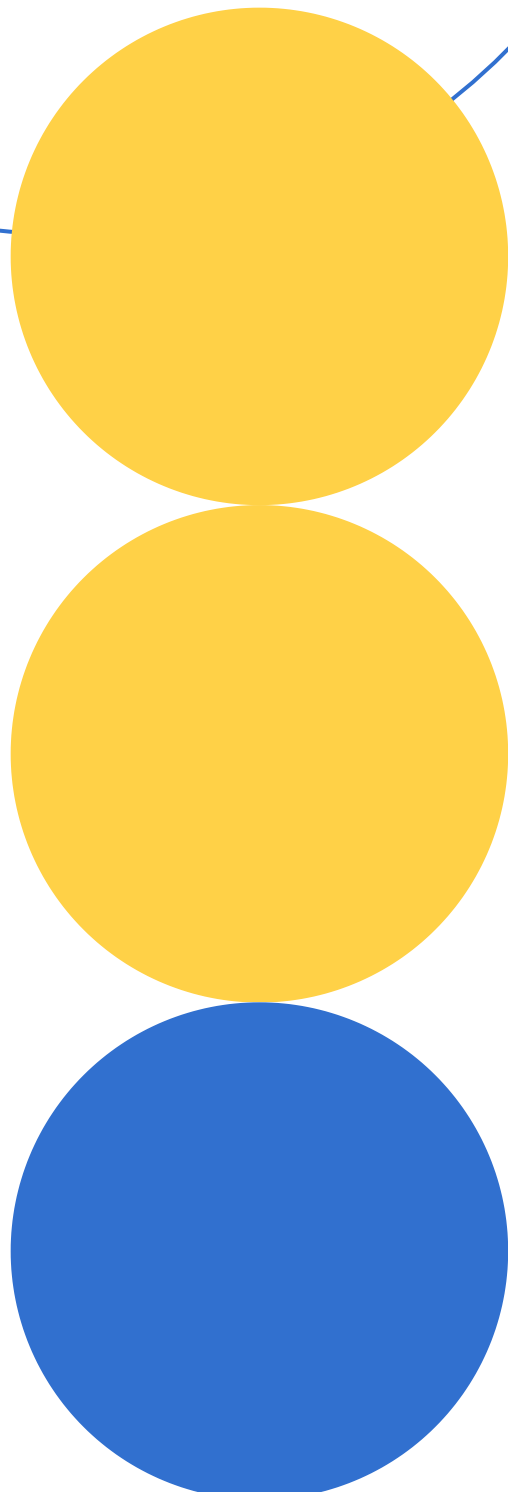
DDoS detector

- effettuare dei test bare metal
- aggiungere una threshold globale
- whitelist e blacklist
- gestione dinamica del numero degli IP controllabili



Anti scan

- effettuare dei test bare metal
- modi più intelligenti per rilevare uno scan
- ottimizzazione per grandi reti



Armillotta Michele +
De Divitiis Edoardo
Raffaelli Andrea

Grazie per
l'attenzione !

