ROMA TRE
UNIVERSITÀ DEGLI STUDI

Realizzazione di un sistema di rilevazione e prevenzione delle intrusioni con Snort

Anno Accademico 2021/2022

Relatore
Prof. Maurizio Patrignani

Correlatore
Ing. Federico Lommi

Laureanda
Allegra Strippoli

Introduzione

Firewall

Il firewall è uno **strumento di difesa che implementa delle politiche di sicurezza basate su regole** e permette di bloccare il traffico non autorizzato.

Criticità del firewall

1. Regole permissive possono lasciare falle di sicurezza.
2. Non è capace di adattarsi autonomamente nel caso in cui si verifichino attacchi.
3. Non distingue i protocolli dei livelli applicativi.
4.

Intrusion Detection System

Un **IDS** è un dispositivo software o hardware **utilizzato per identificare attività anomale**, accessi non autorizzati a un computer o a una rete di computer.

Intrusion Prevention System

Un **IPS** è un dispositivo **utilizzato per prevenire e contrastare attacchi** in rete.

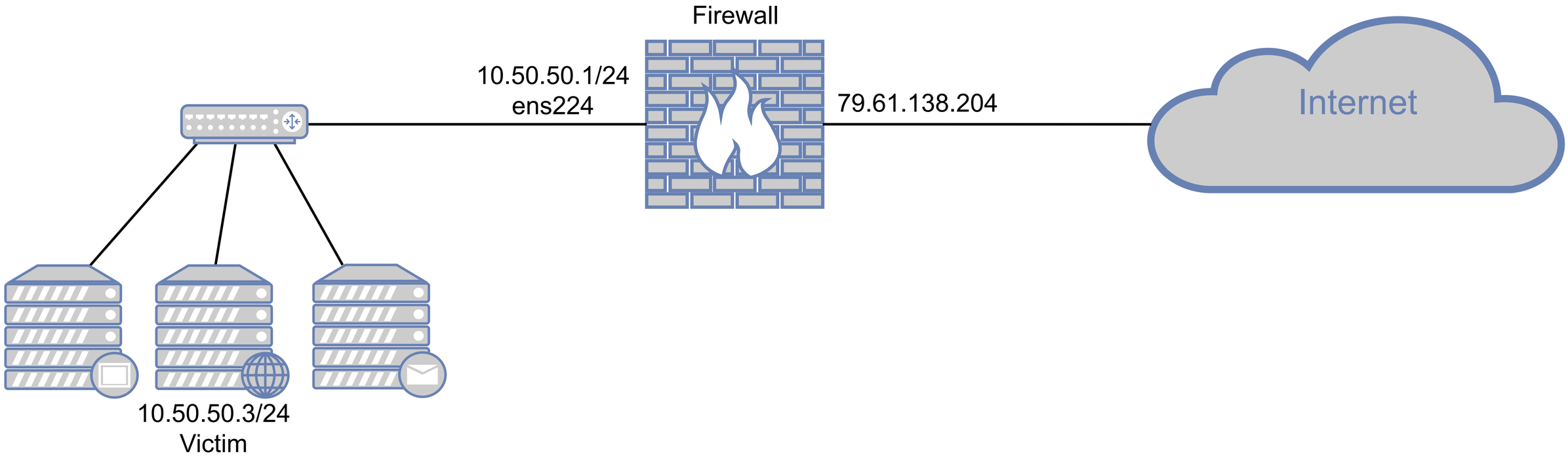
Scopo di un IDS/IPS

Un sistema IDS/IPS:

- Cattura e analizza pacchetti,
- Segnala attività sospette all’amministratore,
- Previene attacchi.

La rete

La rete


Firewall
10.50.50.1/24
ens224
79.61.138.204
Internet
10.50.50.3/24
Victim

Obiettivo

Elevare gli standard di sicurezza della rete.

Come?

Introducendo un sistema di rilevazione e prevenzione delle intrusioni (IDS/IPS).


SNORT®

Snort

un IDS/IPS

Snort è un software open source rule-based.

Può **generare log e alert** che avvisano gli utenti, oppure può **intraprendere azioni di difesa** bloccando il transito di pacchetti sospetti.

Le regole di Snort

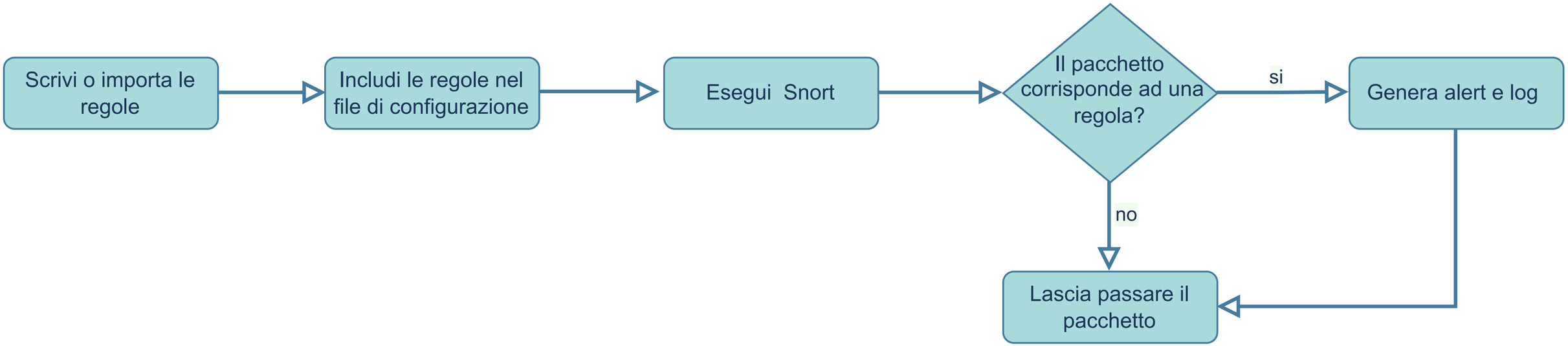
Azione	Protocollo	IP mittente	Porta mittente	Direzione	IP destinazione	Porta destinazione	Opzione
Alert Drop Reject	TCP UDP ICMP	ANY	ANY	→	ANY	ANY	Msg Sid Rev
Header							Options

alert TCP any any → $HOME_NET 22 (msg:“SSH detected”; sid:10000001; rev:001;)

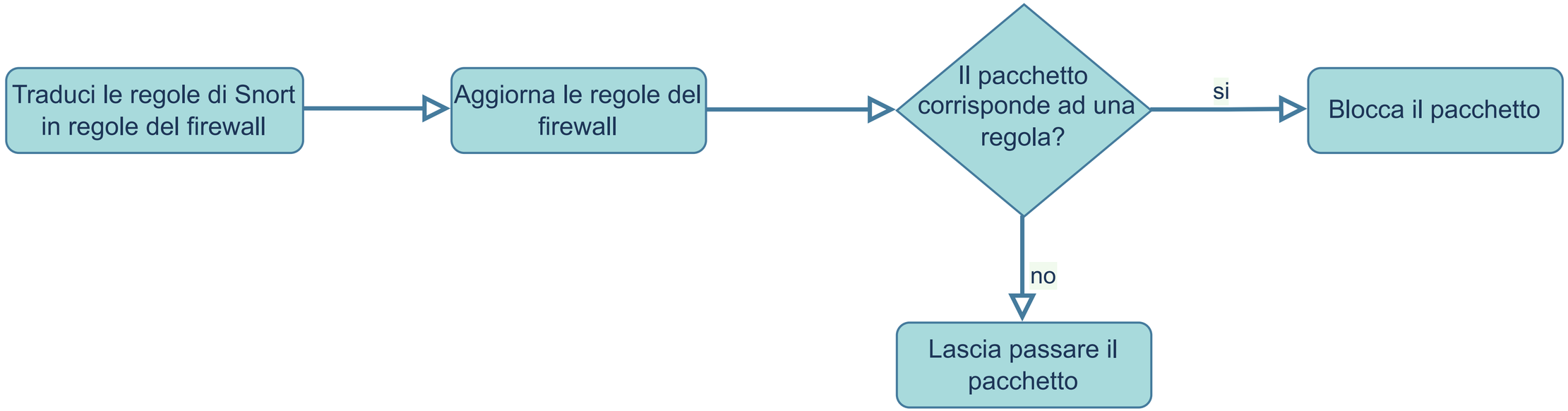
Modalità di esecuzione di Snort

- Sniffer mode
- Packet logging mode
- IDS mode
- IPS con FwSnort

IDS mode

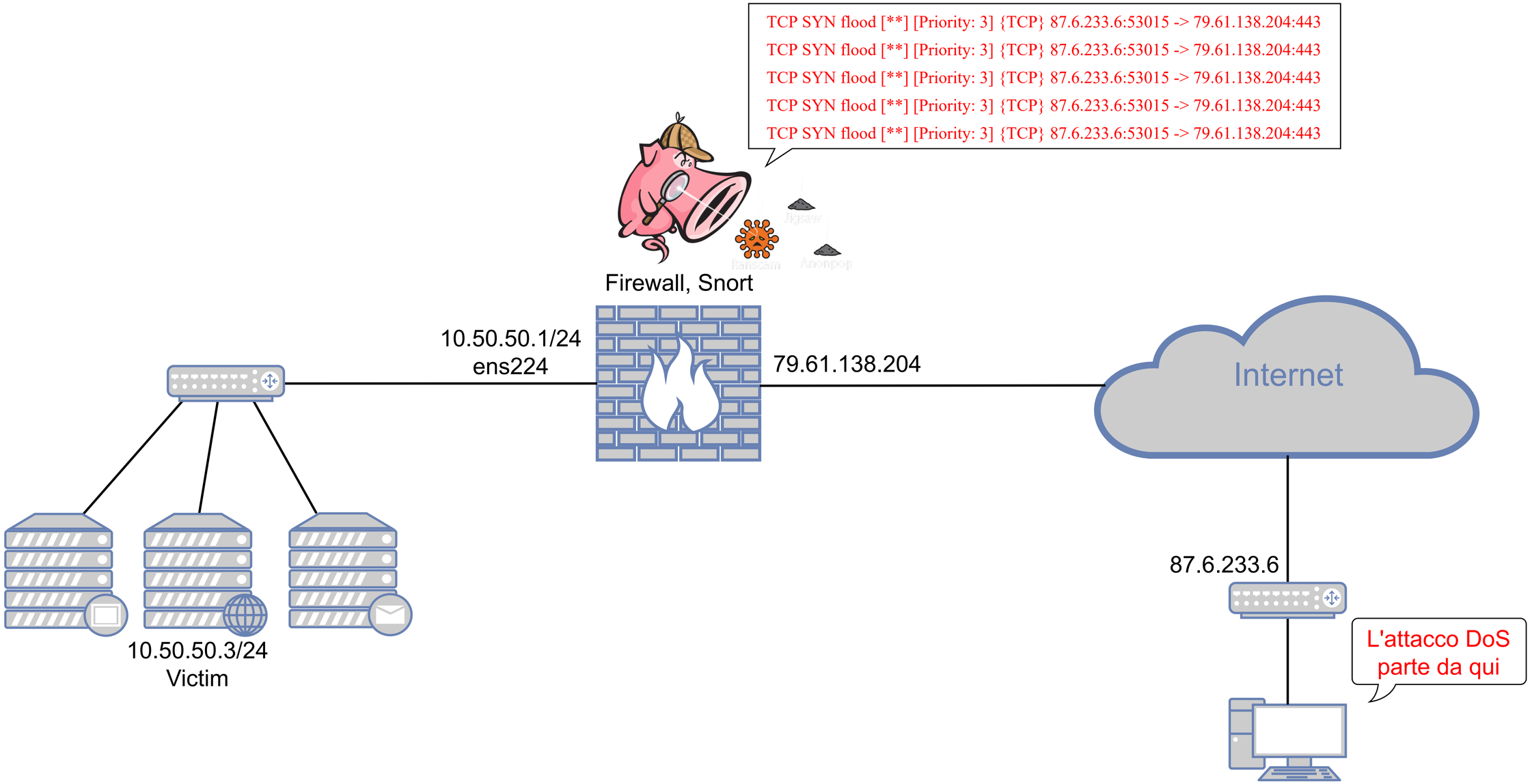

Scrivi o importa le regole
Includi le regole nel file di configurazione
Esegui Snort
Il pacchetto corrisponde ad una regola?
si
Genera alert e log
no
Lascia passare il pacchetto

IPS con FwSnort



Verifiche funzionali

Simulazione attacco DoS



Altre verifiche

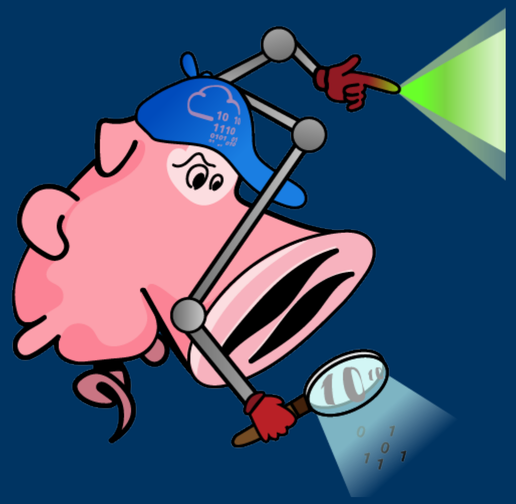
- Analisi del traffico sulle porte del web server.
- Scan delle porte con Nmap.

Conclusioni

Sviluppi futuri

La rete ora è più sicura, ma…

- È possibile aumentare il livello di modularità introducendo un’altra macchina.
- Da FwSnort a Inline mode.
- Ampliare il panorama di test.
- Fornire delle statistiche su falsi positivi e negativi.



Grazie per l’attenzione