Gestione di Reti a.a 2024/2025

Relazione progetto

Candidati: Ferrante Luca [n° 654430]
Data consegna: 06/06/2025

Prerequisiti

1. Aver installato la libreria ***libndpi*** (*brew install ndpi*);
2. Aver installato la libreria ***netsnmp*** (*brew install net-snmp*);
3. Aver installato la libreria ***rrdtool*** (*brew install rrdtool*)*;*
4. Aver installato il compilatore ***gcc*** (*brew install gcc*).

Descrizione

Questo tool è progettato per recuperare informazioni su dispositivi di rete remoti tramite il protocollo SNMP (Simple Network Management Protocol), con l'ausilio di Shodan per l'individuazione preliminare degli host esposti e accessibili.

1. **Scansione e Identificazione Dispositivi SNMP**:
    - Attraverso shodan.io è possibile identificare dispositivi remoti accessibili pubblicamente che espongono il servizio SNMP.
    - Una volta individuato un target e passato come parametro al tool, viene stabilita una connessione SNMP per l'interrogazione dei dati di traffico.
2. **Raccolta Dati SNMP**:
    - Estrae informazioni da OID rilevanti (nel mio caso ifOutOctets).
    - I dati raccolti vengono normalizzati e strutturati per l'analisi (gestendo anche un possibile overflow dei contatori a 32 bit).
3. **Algoritmo di Similarità del Traffico**:
    - Applica un algoritmo di similarità per confrontare i pattern di traffico tra le diverse porte.
    - Identifica le interfacce che mostrano comportamenti simili nel tempo.
4. **Output**:
    - Fornisce un report con:
        - Lista delle interfacce monitorate.
        - Coppie di porte con traffico simile.

Struttura e logica progetto

Il mio progetto è basato su un file principale: "***port_similarity.c***" che contiene tutta la logica del tool. Ho usufruito di tre librerie per implementare il tutto:

- ➔ ***net-snmp***: usata per inizializzare la sessione SNMP e costruire gli SNMP PDU per fare polling al SNMP agent e recuperare le informazioni su *ifOutOctets*;
- ➔ ***rrdtool***: usato per immagazzinare le informazioni raccolte in un database a sequenze temporali. Invece di creare un unico file .rrd contenente molteplici Data Source (DS) — uno per ciascuna interfaccia rilevata tramite SNMP sull'agent remoto — ho preferito adottare un approccio modulare, generando un file .rrd separato per ogni interfaccia. Questo mi ha consentito una gestione più semplice e una maggiore flessibilità nell'analisi e visualizzazione dei dati relativi alle singole porte.

➔ ***ndpi***: usata principalmente per applicare l'algoritmo di similarità tra bin (distanza di Euclide) (https://github.com/ntop/nDPI).

È presente anche un altro file "***gentest.sh***" che rappresenta un piccolo script per generare 5 interfacce di test.

Come funziona?

```
Usage: port_similarity -h <hostname> | -l | -c <basedir> [-a <alpha>][-t <threshold>]
                                  [-e <end>][-s <start>][-S <step][-v][-z]
-e <end>       | RRD end time. Default now
-s <start>     | RRD start time. Default now-1d
-h <hostname>  | Hostname or IP address of the agent
-c <basedir>   | Analyze similarity in RRD files in specified basedir (without SNMP polling)-t <threshold> | Similarity threshol
d. Default 100 (0 == alike)
-l             | Use localhost instead of specifying hostname (127.0.0.1)
-S <step>      | Set RRD step. Valid range >0. Default 60
-v             | Verbose
-z             | Skip zero RRDs during comparison


Example: port_similarity -l


Goal: find similar port on localhost SNMP manager
```

A seconda delle opzioni specificate è possibile avere comportamenti diversi del programma. I principali sono:

- *-l* => con cui è possibile interrogare un SNMP agent installato sulla propria macchina;
- *-h* => con cui è possibile interrogare un SNMP agent installato su una macchina remota;
- *-c* => con cui è possibile passare una directory contenente dei file .rrd e applicare direttamente l'analisi di similarità (applica *rrd_similarity* di nDPI).

Per le prime due opzioni, all'avvio, il tool avvierà un thread che farà **polling** al SNMP agent scelto. Per avere dati sostanziosi è consigliato aspettare 20/30 minuti in modo tale da poter popolare i file rrd. Per interrompere il polling basta mandare un segnale (CTRL-C) e successivamente viene applicato l'algoritmo di similarità sui valori registrati e viene stampato un report (più o meno dettagliato a seconda delle opzioni passate all'avvio).

Istruzioni compilazione e esecuzione

Attraverso il Makefile che ho creato è possibile compilare il tutto attraverso il comando ***make***: viene prima compilata la libreria ndpi, poi vengono create le cartelle */test/* e */rrds/* (rispettivamente la prima contiene i file rrd per il test, la seconda contiene i file rrd degli host contattati) e infine viene compilato il tool.

Per quanto riguarda l'esecuzione:

- ***./port_similarity -h <hostname>***: permette di eseguire il tool con un SNMP agent a vostra scelta.
- ***make run-remote***: permette di eseguire il tool con un SNMP agent già individuato su shodan.io;

- ***make run-local***: permette di eseguire il tool con un SNMP agent installato sulla propria macchina;
- ***make run-test***: permette di eseguire il tool (solo algoritmo similarità) sulla cartella *test/*.

Per un eventuale pulizia dei file .o e altro basta digitare ***make clean***.

Testing

Ho testato il tool andando a scegliere due SNMP agent su ***https://shodan.io*** (obiettivo principale: testare la connessione SNMP all'agent e controllare il corretto recupero dei dati). Nella prima immagine è possibile notare come tra le interfacce rilevate tramite SNMP non ci sono comportamenti simili.

```
Found 0 (0.000 %) similar RRDs / 78 zero alike RRDs [num_rrds: 22]
src/rrds/200.58.174.254/1.rrd   1472302.6       5508852.5
src/rrds/200.58.174.254/2.rrd   0.0     0.0
src/rrds/200.58.174.254/3.rrd   25525020.0      29019320.0
src/rrds/200.58.174.254/4.rrd   0.0     0.0
src/rrds/200.58.174.254/5.rrd   3611295.2       13512230.0
src/rrds/200.58.174.254/6.rrd   0.0     0.0
src/rrds/200.58.174.254/7.rrd   0.0     0.0
src/rrds/200.58.174.254/8.rrd   0.0     0.0
src/rrds/200.58.174.254/9.rrd   24268090.0      26491224.0
src/rrds/200.58.174.254/10.rrd  3105735.5       11620598.0
src/rrds/200.58.174.254/11.rrd  26570886.0      27863484.0
src/rrds/200.58.174.254/12.rrd  607501.9        2273064.0
src/rrds/200.58.174.254/13.rrd  802887.0        3004128.0
src/rrds/200.58.174.254/14.rrd  0.0     0.0
src/rrds/200.58.174.254/15.rrd  3250943.2       12163916.0
src/rrds/200.58.174.254/16.rrd  0.0     0.0
src/rrds/200.58.174.254/17.rrd  0.0     0.0
src/rrds/200.58.174.254/18.rrd  0.0     0.0
src/rrds/200.58.174.254/19.rrd  0.0     0.0
src/rrds/200.58.174.254/20.rrd  0.0     0.0
src/rrds/200.58.174.254/21.rrd  0.0     0.0
src/rrds/200.58.174.254/22.rrd  0.0     0.0
```

1. Esempio senza similarità: https://www.shodan.io/host/200.58.174.254
(HP V1910-16G Switch Software Version 5.20)

Nella seconda immagine, invece, tra le tante interfacce individuate (96), sono stati rilevati comportamenti simili se non "identici" tra coppie di porte: il tool ha evidenziato che **solo il**

7.8% mostra traffico differenziato, mentre il resto dei file suggerisce traffico identico o fortemente simile.

```
rrds/193.37.138.128/43.rrd [1395374.0/9736766.0]  - rrds/193.37.138.128/44.rrd [1395373.4/9736762.0] are similar [30.0]
rrds/193.37.138.128/62.rrd [1395638.8/9738614.0]  - rrds/193.37.138.128/70.rrd [1395639.2/9738618.0] are similar [22.0]
rrds/193.37.138.128/62.rrd [1395638.8/9738614.0]  - rrds/193.37.138.128/72.rrd [1395639.2/9738618.0] are similar [22.0]
rrds/193.37.138.128/62.rrd [1395638.8/9738614.0]  - rrds/193.37.138.128/76.rrd [1395639.2/9738618.0] are similar [22.0]
rrds/193.37.138.128/62.rrd [1395638.8/9738614.0]  - rrds/193.37.138.128/77.rrd [1395639.2/9738618.0] are similar [22.0]
rrds/193.37.138.128/62.rrd [1395638.8/9738614.0]  - rrds/193.37.138.128/80.rrd [1395639.2/9738618.0] are similar [22.0]
rrds/193.37.138.128/62.rrd [1395638.8/9738614.0]  - rrds/193.37.138.128/81.rrd [1395639.2/9738617.0] are similar [21.0]
rrds/193.37.138.128/62.rrd [1395638.8/9738614.0]  - rrds/193.37.138.128/84.rrd [1395639.2/9738618.0] are similar [22.0]
rrds/193.37.138.128/62.rrd [1395638.8/9738614.0]  - rrds/193.37.138.128/85.rrd [1395639.2/9738618.0] are similar [22.0]
rrds/193.37.138.128/62.rrd [1395638.8/9738614.0]  - rrds/193.37.138.128/89.rrd [1395639.1/9738616.0] are similar [15.0]
rrds/193.37.138.128/62.rrd [1395638.8/9738614.0]  - rrds/193.37.138.128/93.rrd [1395639.2/9738618.0] are similar [22.0]
rrds/193.37.138.128/62.rrd [1395638.8/9738614.0]  - rrds/193.37.138.128/96.rrd [1395639.1/9738616.0] are similar [17.0]
rrds/193.37.138.128/69.rrd [798395.9/5571118.5]  - rrds/193.37.138.128/75.rrd [798395.9/5571118.5] are alike [0.0]
rrds/193.37.138.128/70.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/72.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/70.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/76.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/70.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/77.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/70.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/80.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/70.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/81.rrd [1395639.2/9738617.0] are similar [1.0]
rrds/193.37.138.128/70.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/84.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/70.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/85.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/70.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/89.rrd [1395639.1/9738616.0] are similar [7.0]
rrds/193.37.138.128/70.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/93.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/70.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/96.rrd [1395639.1/9738616.0] are similar [5.0]
rrds/193.37.138.128/72.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/76.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/72.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/77.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/72.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/80.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/72.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/81.rrd [1395639.2/9738617.0] are similar [1.0]
rrds/193.37.138.128/72.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/84.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/72.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/85.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/72.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/89.rrd [1395639.1/9738616.0] are similar [7.0]
rrds/193.37.138.128/72.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/93.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/72.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/96.rrd [1395639.1/9738616.0] are similar [5.0]
rrds/193.37.138.128/76.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/77.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/76.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/80.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/76.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/81.rrd [1395639.2/9738617.0] are similar [1.0]
rrds/193.37.138.128/76.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/84.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/76.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/85.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/76.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/89.rrd [1395639.1/9738616.0] are similar [7.0]
rrds/193.37.138.128/76.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/93.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/76.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/96.rrd [1395639.1/9738616.0] are similar [5.0]
rrds/193.37.138.128/77.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/80.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/77.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/81.rrd [1395639.2/9738617.0] are similar [1.0]
rrds/193.37.138.128/77.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/84.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/77.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/85.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/77.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/89.rrd [1395639.1/9738616.0] are similar [7.0]
rrds/193.37.138.128/77.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/93.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/77.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/96.rrd [1395639.1/9738616.0] are similar [5.0]
rrds/193.37.138.128/80.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/81.rrd [1395639.2/9738617.0] are similar [1.0]
rrds/193.37.138.128/80.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/84.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/80.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/85.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/80.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/89.rrd [1395639.1/9738616.0] are similar [7.0]
rrds/193.37.138.128/80.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/93.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/80.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/96.rrd [1395639.1/9738616.0] are similar [5.0]
rrds/193.37.138.128/81.rrd [1395639.2/9738617.0]  - rrds/193.37.138.128/84.rrd [1395639.2/9738618.0] are similar [1.0]
rrds/193.37.138.128/81.rrd [1395639.2/9738617.0]  - rrds/193.37.138.128/85.rrd [1395639.2/9738618.0] are similar [1.0]
rrds/193.37.138.128/81.rrd [1395639.2/9738617.0]  - rrds/193.37.138.128/89.rrd [1395639.1/9738616.0] are similar [6.0]
rrds/193.37.138.128/81.rrd [1395639.2/9738617.0]  - rrds/193.37.138.128/93.rrd [1395639.2/9738618.0] are similar [1.0]
rrds/193.37.138.128/81.rrd [1395639.2/9738617.0]  - rrds/193.37.138.128/96.rrd [1395639.1/9738616.0] are similar [4.0]
rrds/193.37.138.128/84.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/85.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/84.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/89.rrd [1395639.1/9738616.0] are similar [7.0]
rrds/193.37.138.128/84.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/93.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/84.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/96.rrd [1395639.1/9738616.0] are similar [5.0]
rrds/193.37.138.128/85.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/89.rrd [1395639.1/9738616.0] are similar [7.0]
rrds/193.37.138.128/85.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/93.rrd [1395639.2/9738618.0] are alike [0.0]
rrds/193.37.138.128/85.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/96.rrd [1395639.1/9738616.0] are similar [5.0]
rrds/193.37.138.128/89.rrd [1395639.1/9738616.0]  - rrds/193.37.138.128/93.rrd [1395639.2/9738618.0] are similar [7.0]
rrds/193.37.138.128/89.rrd [1395639.1/9738616.0]  - rrds/193.37.138.128/96.rrd [1395639.1/9738616.0] are similar [2.0]
rrds/193.37.138.128/93.rrd [1395639.2/9738618.0]  - rrds/193.37.138.128/96.rrd [1395639.1/9738616.0] are similar [5.0]
Found 68 (0.738 %) similar RRDs / 253 zero alike RRDs [num_rrds: 96]
```

2. Esempio con similarità: https://www.shodan.io/host/193.37.138.128
(Cisco IOS Software, Catalyst 4500 L3 Switch Software)

Ho fatto ulteriori test in locale (obiettivo principale: controllare la corretta applicazione dell'algoritmo di similarità):

1. Attraverso "***gentest.sh***", genero dei valori di ifOutOctets che successivamente vengono inseriti all'interno di file rrd.

```
# Valori iface1
OUT1=$((2000000 + $i * 700))

# iface2 con una piccola variazione casuale
OUT2=$(($OUT1 + RANDOM % 70))

#same per iface3 e 4

OUT3=$((100000 + $i * 500))

OUT4=$(($OUT3 + RANDOM % 100))

#metto una if totalmente uguale

OUT5=$OUT2
```

Più precisamente, genero *OUT1* e *OUT3* basandomi sul valore del ciclo for e successivamente creo *OUT2* e *OUT4* con una piccola variazione casuale. Infine, inserisco genero *OUT5* in maniera totalmente uguale a *OUT2*.

```
test/1.rrd [0.0/1.1]  - test/3.rrd [0.0/0.8] are similar [40.0]
test/1.rrd [0.0/1.1]  - test/2.rrd [0.0/1.1] are similar [3.0]
test/1.rrd [0.0/1.1]  - test/5.rrd [0.0/1.1] are similar [3.0]
test/1.rrd [0.0/1.1]  - test/4.rrd [0.0/0.7] are similar [45.0]
test/3.rrd [0.0/0.8]  - test/2.rrd [0.0/1.1] are similar [43.0]
test/3.rrd [0.0/0.8]  - test/5.rrd [0.0/1.1] are similar [43.0]
test/3.rrd [0.0/0.8]  - test/4.rrd [0.0/0.7] are similar [5.0]
test/2.rrd [0.0/1.1]  - test/5.rrd [0.0/1.1] are alike [0.0]
test/2.rrd [0.0/1.1]  - test/4.rrd [0.0/0.7] are similar [48.0]
test/5.rrd [0.0/1.1]  - test/4.rrd [0.0/0.7] are similar [48.0]
Found 10 (40.000 %) similar RRDs / 0 zero alike RRDs [num_rrds: 5]
test/1.rrd      0.0     1.1
test/3.rrd      0.0     0.8
test/2.rrd      0.0     1.1
test/5.rrd      0.0     1.1
test/4.rrd      0.0     0.7
```

Il tool mostra come le interfacce 1 / 2 / 5 e 3 / 4 siano molto simili (minore è il valore tra parentesi quadre, maggiore è la similarità), se non identiche (caso 2-5), il che garantisce un corretto funzionamento dell'algoritmo.

2. Ho installato un agent SNMP sulla mia macchina locale (https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-an-snmp-daemon-and-client-on-ubuntu-18-04) e ho fatto girare il tool facendo polling SNMP in localhost (chiaramente con step minore per non attendere troppo tempo).

```
Found 0 (0.000 %) similar RRDs / 136 zero alike RRDs [num_rrds: 21]
rrds/127.0.0.1/1.rrd    192531440.0     213594288.0
rrds/127.0.0.1/2.rrd    0.0     0.0
rrds/127.0.0.1/3.rrd    0.0     0.0
rrds/127.0.0.1/4.rrd    0.0     0.0
rrds/127.0.0.1/5.rrd    0.0     0.0
rrds/127.0.0.1/6.rrd    0.0     0.0
rrds/127.0.0.1/7.rrd    0.0     0.0
rrds/127.0.0.1/8.rrd    0.0     0.0
rrds/127.0.0.1/9.rrd    0.0     0.0
rrds/127.0.0.1/10.rrd   0.0     0.0
rrds/127.0.0.1/11.rrd   177592496.0     211376656.0
rrds/127.0.0.1/12.rrd   0.0     0.0
rrds/127.0.0.1/13.rrd   0.0     0.0
rrds/127.0.0.1/14.rrd   44430432.0      130799616.0
rrds/127.0.0.1/15.rrd   0.0     0.0
rrds/127.0.0.1/16.rrd   0.0     0.0
rrds/127.0.0.1/17.rrd   0.0     0.0
rrds/127.0.0.1/18.rrd   0.0     0.0
rrds/127.0.0.1/19.rrd   0.0     0.0
rrds/127.0.0.1/20.rrd   14810154.0      78367976.0
rrds/127.0.0.1/21.rrd   0.0     0.0
```