THE ITALIAN RESEARCH & EDUCATION NETWORK

Consortium GARR

argus

Roberto Cecchini & Simona Venuti

Tutorial Workshop GARR 2014, Roma, 2-4 Dicembre

argus

- http://www.qosient.com/argus
- Sniffer di flussi invece che di pacchetti (tcpdump)
- Architettura client/server:
  - **argus** legge i pacchetti dalla rete (o netflow o un file pcap) e scrive su un file o socket;
  - **ra** (o un altro client) legge l'output di **argus** e traduce i dati in forma leggibile
  - la sintassi per filtrare i dati è molto simile a quella di **tcpdump**

Collocazione

- Ovviamente dipende dalla topologia della rete e da cosa volete tracciare
- NAT?
- firewall?
- router configuration?

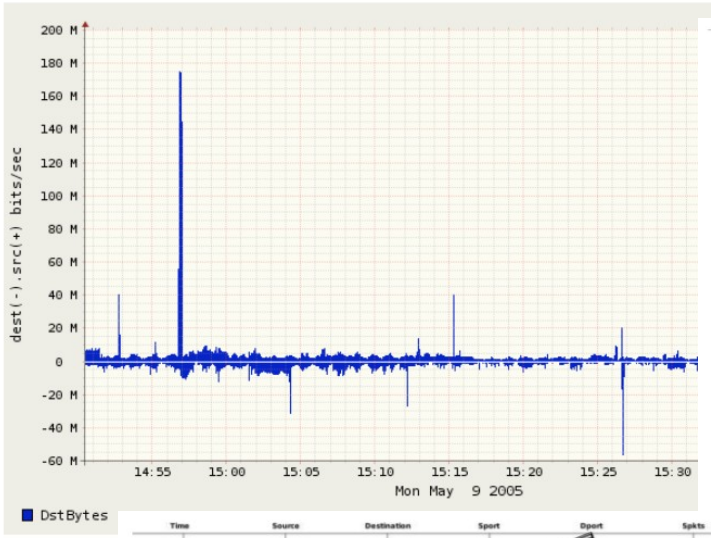
Volume dati

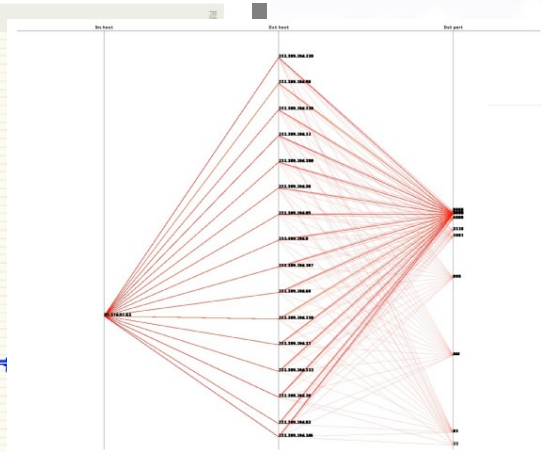
- L'output di argus può essere compresso (circa il 50%)
  - leggibile dai client direttamente
- In un ambiente medio qualche GB al giorno
- Che velocità?

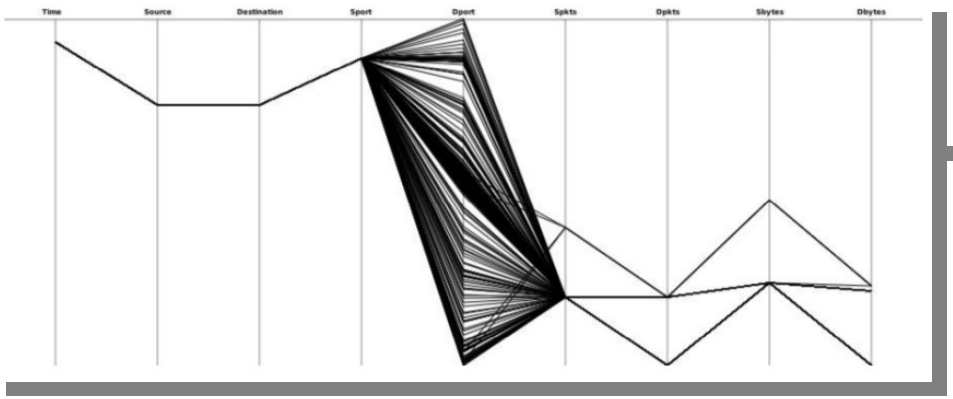
Client

- **ra**
- **racluster**: raggruppa dati
- **racount**: totali pacchetti e byte
- **ragraph, raplot**: GNUPlot, Mathematica, MatLab, cvs, AfterGlow, PicViz, etc...
- **rasort**
- **rahosts**

Grafici


200 M
180 M
160 M
140 M
120 M
100 M
80 M
60 M
40 M
20 M
0
-20 M
-40 M
-60 M
dest(-).src(+) bits/sec
14:55
15:00
15:05
15:10
15:15
15:20
15:25
15:30
Mon May 9 2005
DstBytes




Time
Source
Destination
Sport
Dport
Spkts
Dpkts
Sbytes
Dbytes

Esempi di uso

- Traffico
  - top talkers
  - packet loss rate
- Connessioni:
  - scansioni
  - SYN flood (DOS)
  - P2P
- Servizi:
  - SMTP anomali
  - DHCP anomali

Esempi

- Traffico da / a una macchina
  - `ra -nr <file> - host 192.168.1.3`
- Top talkers:
  - `racluster -M rmon -m saddr -r <file> -w - | rasort -r - -m bytes`
- Top talkers using port 22
  - `racluster -M rmon -m saddr -r <file> -w - - port 22 | rasort -r - -m bytes`

Esempi

- Porte più utilizzate
  - **racluster -M rmon -m proto sport -r <file>**
- Statistiche per protocollo
  - **racluster -M rmon -m proto -r <file>**
- Traffico per top 10 coppie di host (lungo!)
  - **racluster -M matrix -r <file> -w - | rasort -m bytes -w - | head -10**

Esercizi

- Il file fornito è un estratto da un file reale del 27/11, dalle 15 alle 18
- La rete locale è 10.10.10.0/24
- Il server nat è 10.10.10.3 (non ci sono i dati dei client)
- Domande
  - Chi si e' collegato a 100.0.10.47 alle 16:19?
  - Chi sta usando server DNS esterni?
  - Chi sta facendo P2P?