Gestione di Rete

Luca Deri
deri@ntop.org
luca.deri@di.unipi.it

Riferimenti

Slides Corso: http://luca.ntop.org/
Indirizzo Email: deri@ntop.org
luca.deri@di.unipi.it
Aula Ricevimento: 311 PS
Progetti: https://github.com/lucaderi/sgr
Gruppo Telegram: https://t.me/gestionedirete

Orario Lezioni: Martedi Aula D1 16.15-18
Giovedi Aula A1 9.00-10.45

Panoramica del Corso

- Introduzione ai principali protocolli per il monitoraggio di rete.
- Conoscenza pratica di alcuni casi comuni di monitoraggio e loro risoluzione.
- Panoramica sullo stato dell'arte inclusi gli sviluppi attuali e le ricerche in corso.
- Cybersecurity ed Analisi Dati
- Questo non é un corso solamente teorico

Obiettivi del Corso

- Dare una conoscenza ‘pratica’ della materia estendendo conoscenze di reti esistenti.
- Risolvere assieme problemi comuni di monitoraggio e sicurezza.
- Fare capire cosa succede ’veramente’ nei sistemi di comunicazione (dalla interfaccia utente al cavo di rete).
- Analizzare i dati raccolti tramite algoritmi di analisi numerica in modo da capire veramente cosa stà succedendo in rete.

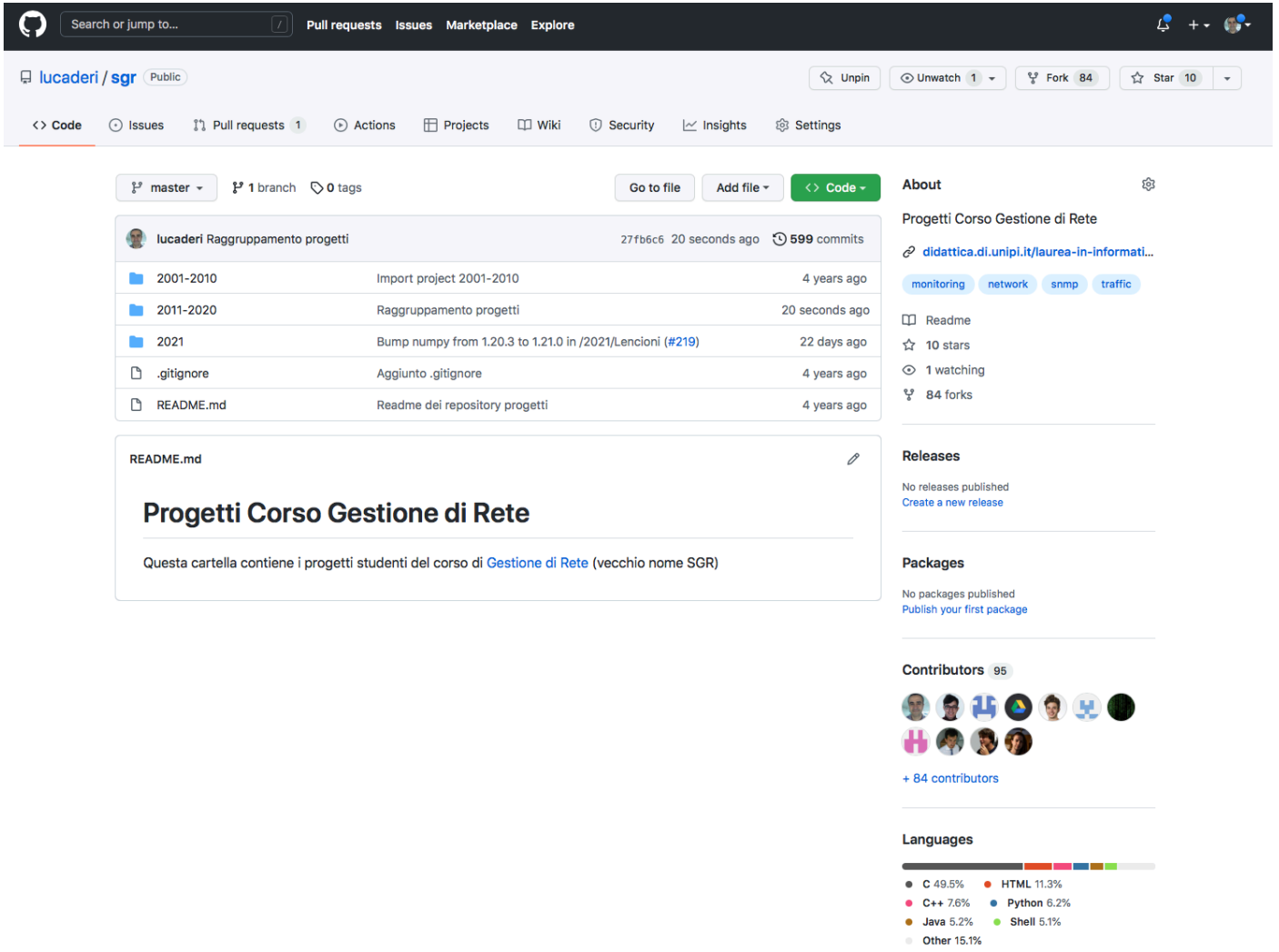
Prerequisiti

- Conoscenza *minima* di come funziona una rete Internet.
- Volontà di imparare come funzionano nella pratica i sistemi di comunicazione.
- Interesse a 'volersi sporcare le mani' a programmare nuovi strumenti per l'analisi accurata del traffico di rete.

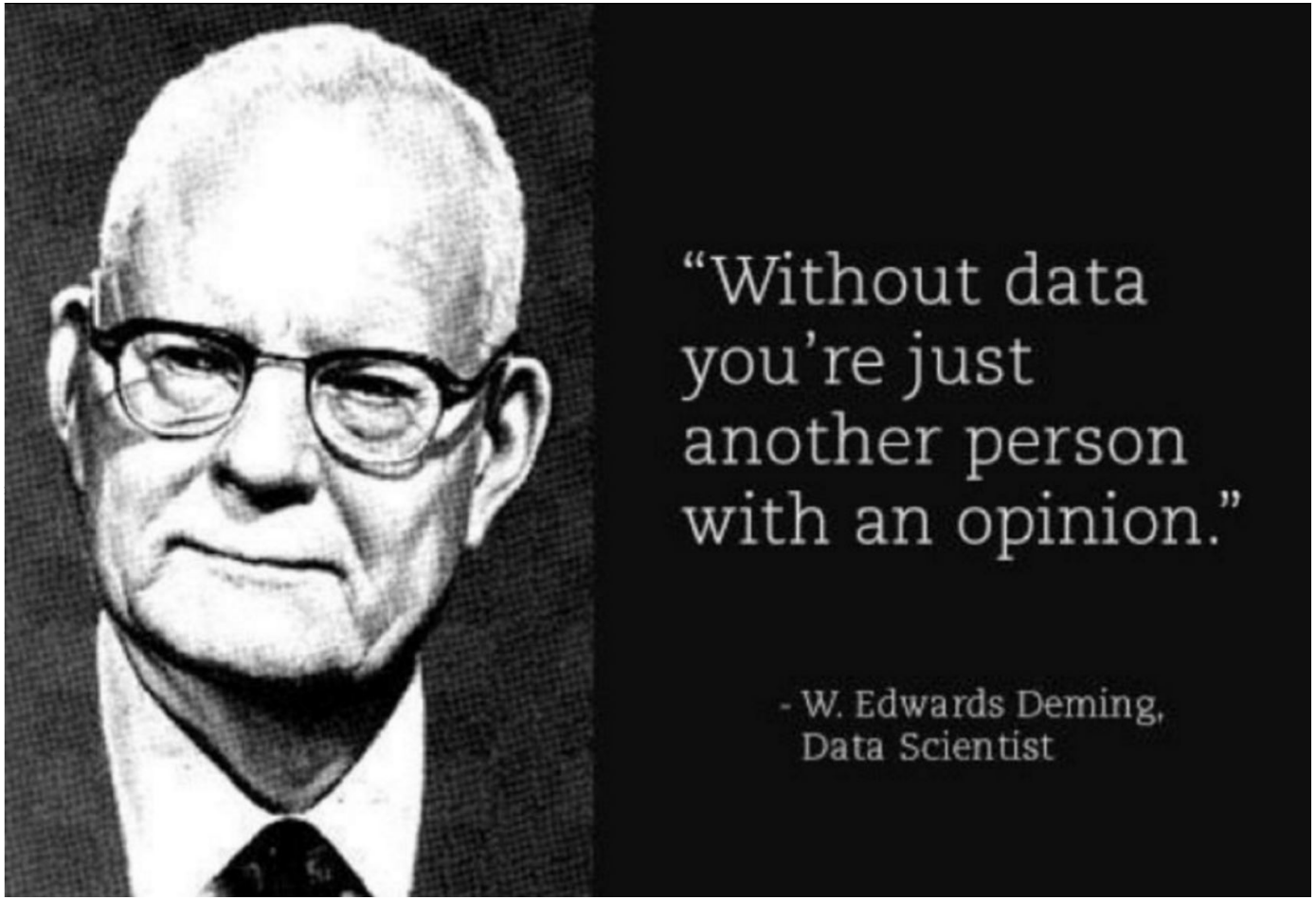
Esame

- Esercizi “in itinere” sugli argomenti trattati (no compitini).
- Breve progetto pratico da realizzare da soli o in coppia e da consegnare su GitHub.
- Orale prevalentemente sulla seconda parte del corso (misura traffico di rete).

https://github.com/lucaderi/sgr



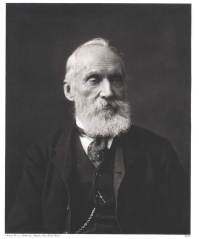
Motivazione [1/2]

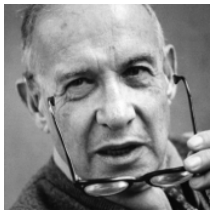


Motivazione [2/2]

- Senza misure non possiamo produrre i risultati attesi, misurare i miglioramenti e quantificare il successo.
- Il traffico di rete non fa eccezione a questa regola.

If you can't measure it, you can't improve it
(Lord Kelvin, 1824 – 1907)

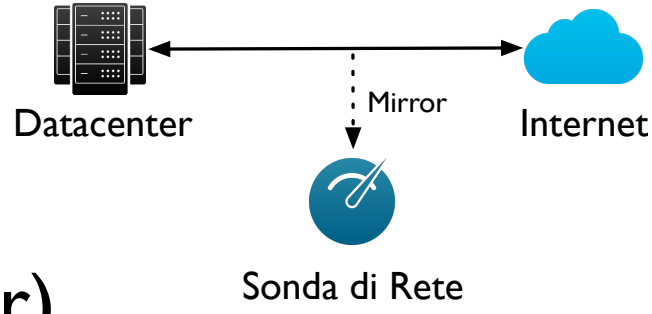




If you can't measure it, you can't manage it
(Peter Drucker, 1909 – 2005)

Come si Misura il Traffico di Rete

1. Individuare un punto della rete dove passa il traffico da analizzare (tipicamente vicino al router).



3. Installazione di una sonda di rete capace di analizzare tale traffico:
   1. Passiva: solo analisi, no modifica/blocco traffico.
   2. Attiva: il traffico attraversa la sonda che può bloccarlo se necessario.

Che Misure di Rete Possiamo Fare?

- Analisi Quantitativa di Traffico
  - Top Talkers (Senders and Receivers)
  - Destinazioni verso/da le quali viene scambiato traffico.
  - Protocolli applicativi utilizzati (Skype, HTTP, Email)
  - Rendicontazione traffico per host.

- Analisi Qualitativa di Traffico
  - Utilizzo di traffico non permessi (es. Tor o VPN anonime).
  - Identificazioni errori ed anomalie di rete che possono causare malfunzionamenti nell'utilizzo dei servizi di rete.

Didattica

1. Teoria (un terzo della durata totale del corso):
   - Introduzione
   - Monitoraggio di reti IP: SNMP.
2. Laboratorio/Pratica (due terzi della durata totale del corso):
   - Introduzione alla misurazione del traffico di rete.
   - Configurazione ed utilizzo pratico di router e sistemi di monitoraggio per piccole reti
   - Strumenti open-source per il monitoraggio di rete e la risoluzione di comuni problemi di rete.
   - Misure utilizzando soluzioni basate SNMP.
   - Flow-based Measurement: NetFlow/IPFIX, sFlow.
   - Misurazione di Rete: casi reali di monitoraggio.
   - Monitoraggio di traffico P2P, VoIP (Voice over IP), wireless.
   - Geolocalizzazione di host in Internet.
   - Visualizzazione dei dati di traffico
   - Memorizzazione delle misure di rete mediante databases efficienti per questi caso d'uso e sistemi per la memorizzazione dei dati di serie temporali
   - Deep packet inspection (DPI) e "host reputation" per la caratterizzazione del traffico di rete applicativo.
   - Monitoraggio degli eventi di sistema utilizzando sysdig ed eBPF
   - Il kernel Linux: stack IP ed il sistema di comunicazione.
   - Monitoraggio di reti mobili 3G/LTE/WiFi e di terminali mobili
   - Memorizzazione dei dati di traffico: RRD, InfluxDB e database no-SQL.
   - Cattura e gestione di traffico ad alta velocità
   - Accelerazione di applicazioni di sicurezza e Linux firewall.
   - Casi pratici di analisi di cybersecurity di rete
   - Algoritmi per l'analisi dei dati di traffico

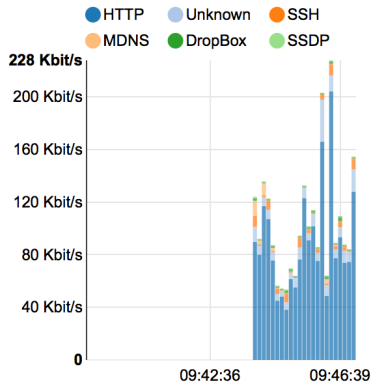
https://esami.unipi.it/esami2/programma.php?c=38036&aa=2021&docente=DERI&insegnamento=&sd=0

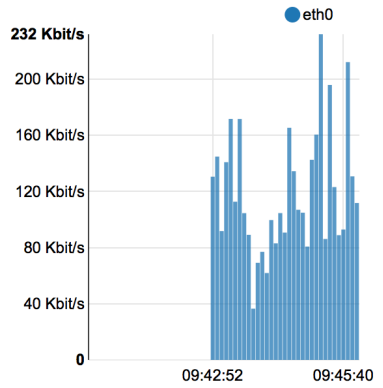
Nuovi Argomenti 2021/22

- Analisi traffico per Cybersecurity
- Algoritmi per l'analisi dei dati
- Rilevazione Anomalie
  - Analisi serie temporali
  - Indicatore di comportamenti inaspettati
  - Utilizzo di tecniche per la rilevazione di anomalie
  - Analisi statistica vs Machine Learning

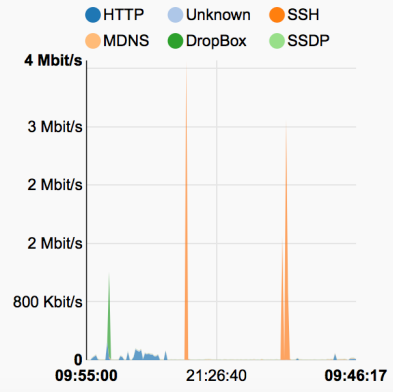
Obiettivo Finale:Visibilità e Sicurezza

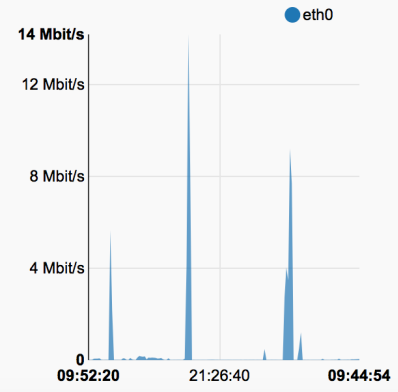
eth0: Top Local Talkers	Actual Traffic
pc-deri.nic.it	122.19 Kbit ↑
192.12.193.127	1.48 Kbit ↓
ninja.nic.it	665.2 bps ↑
pc-lucchesi.nic.it	417.35 bps ↑
mac-raciti.nic.it	294.28 bps ↓
oxcart.nic.it	143.94 bps ↑
shuttle.nic.it	99.16 bps ↓





eth0: Top Remote Destinations	Actual Traffic
host209-190-dynamic.24-79-r.retail.telecomitalia.it	113.26 Kbit ↑
116.31.99.92	6.11 Kbit ↑
Broadcast	1.48 Kbit ↑
192.168.17.87	426.94 bps ↑
192.168.17.255	426.94 bps ↑
192.12.195.255	417.35 bps ↑
ff02::1:fffc:afc2	137.54 bps ↑





Prima di iniziare… [1/3]

Prima di iniziare… [2/3]

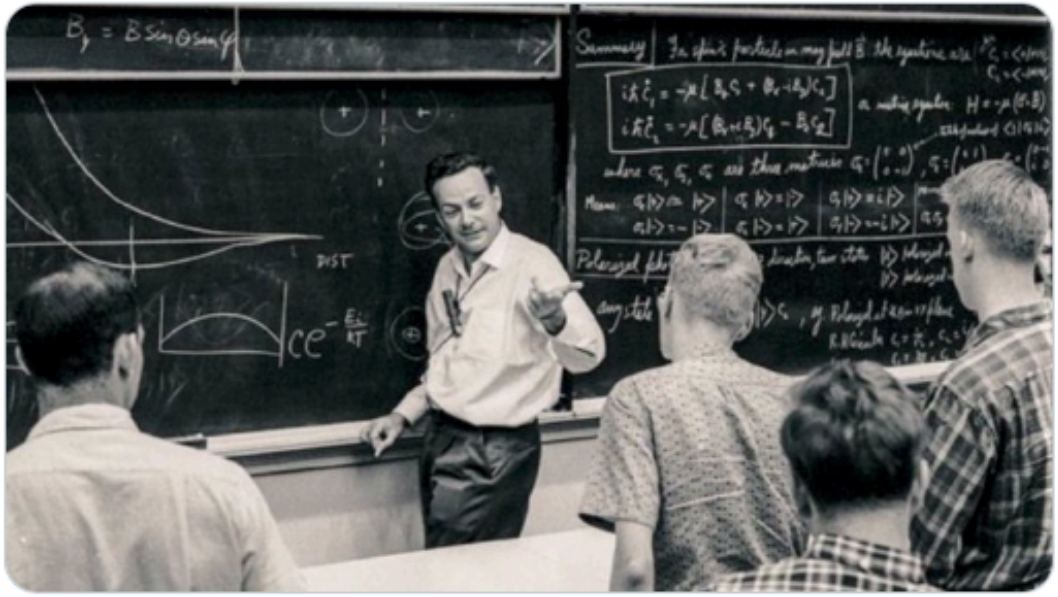
Vala Afshar @ValaAfshar · 9h

Never confuse education with intelligence.

Intelligence isn't the ability to remember and repeat, like they teach you in school.

Intelligence is the ability to learn from experience, solve problems, and use our knowledge to adapt to new situations.

—Professor Richard Feynman



Prima di iniziare… [3/3]