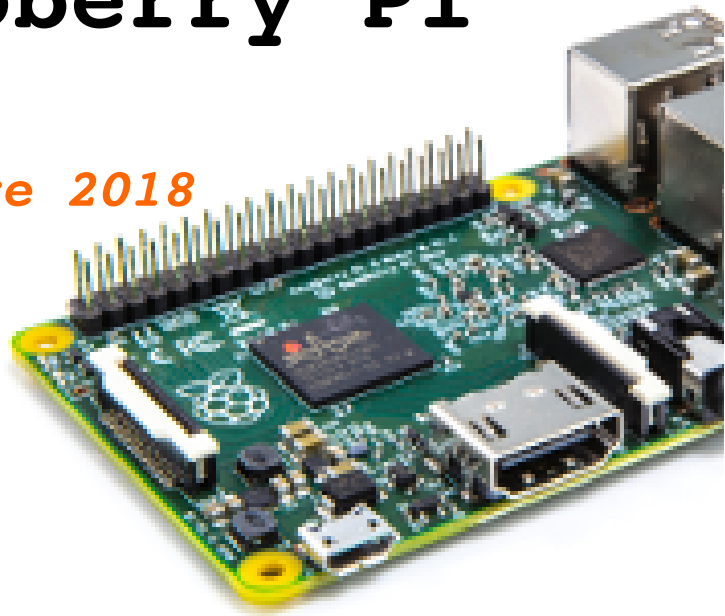
Monitoraggio e penetration testing di reti LAN con Raspberry Pi

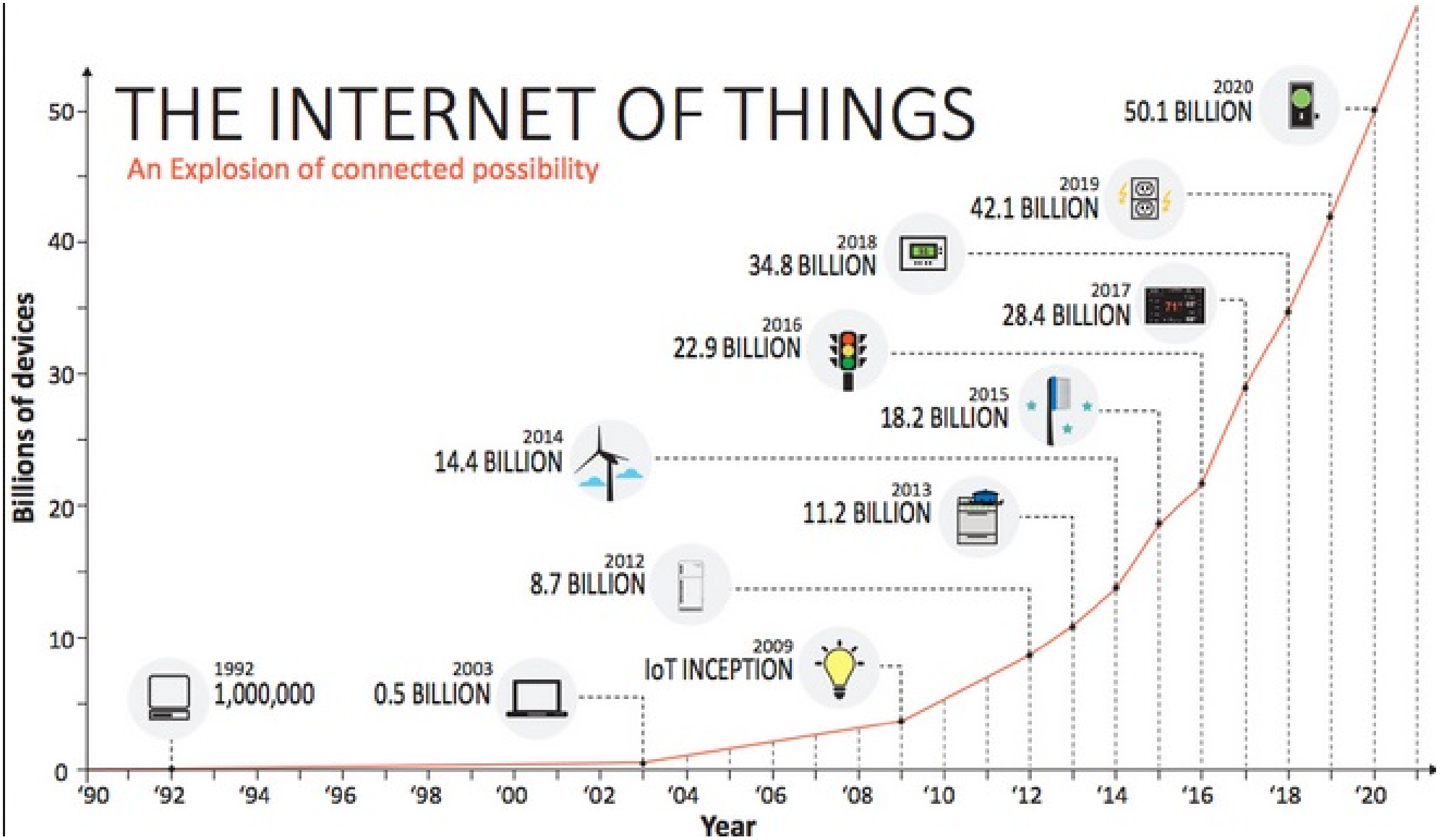
Marco Marcellini — 9 ottobre 2018



STUDIUM GENERALE CIVITATIS PERUSII · A.D. MCCCVIII ·

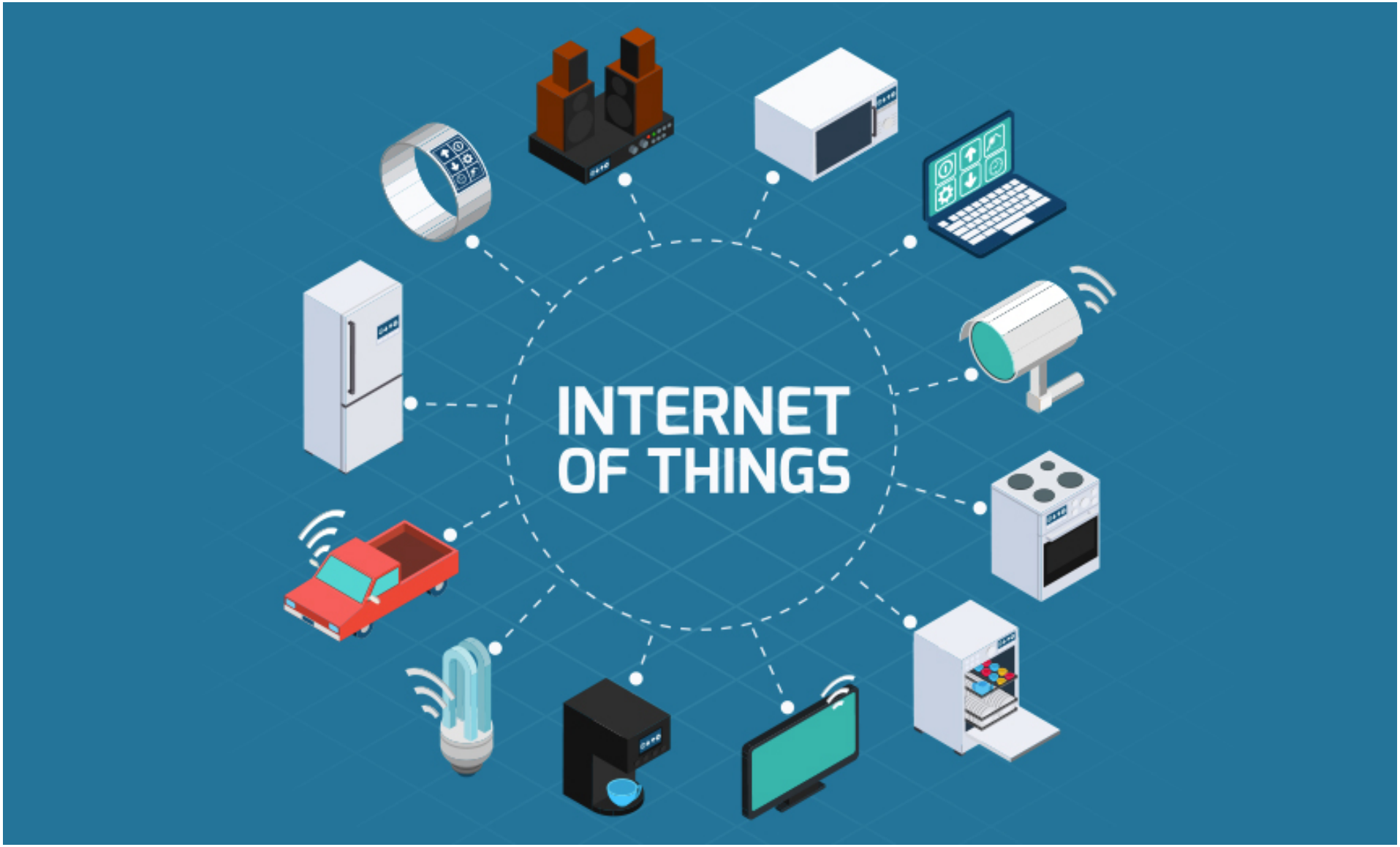
MESE EUROPEO DELLA SICUREZZA INFORMATICA

Evoluzione dell'Internet of Things



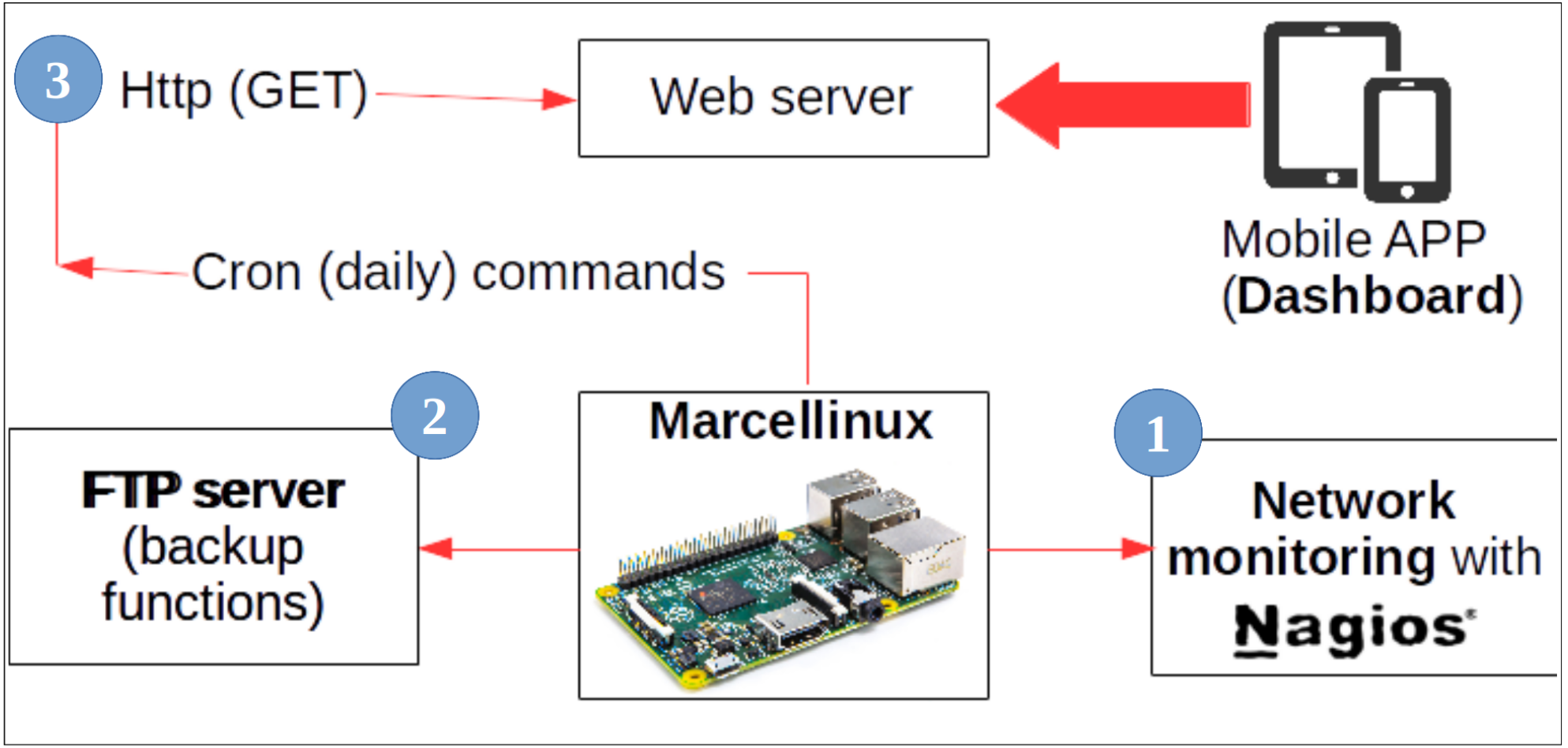
Fonte: http://drrajivdesaimd.com/2016/07/19/internet-of-things-iot/

IoT changes the Cybersecurity Landscape



L’architettura di *Marcellinux*

Figura 6 – Architettura generale del sistema



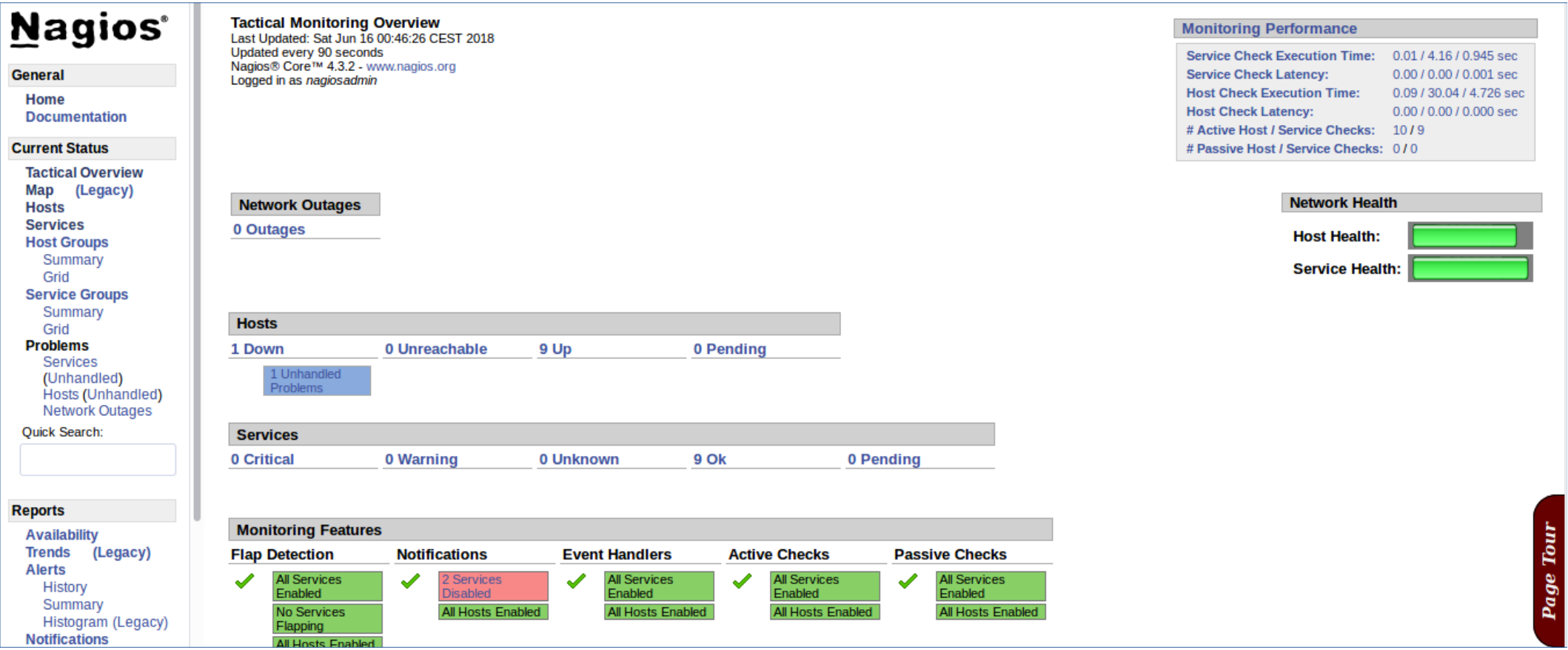
Network monitoring con Nagios®

- Una volta installato Nagios4 dal codice sorgente, sara' sufficiente editare l'appropriato file di configurazione:

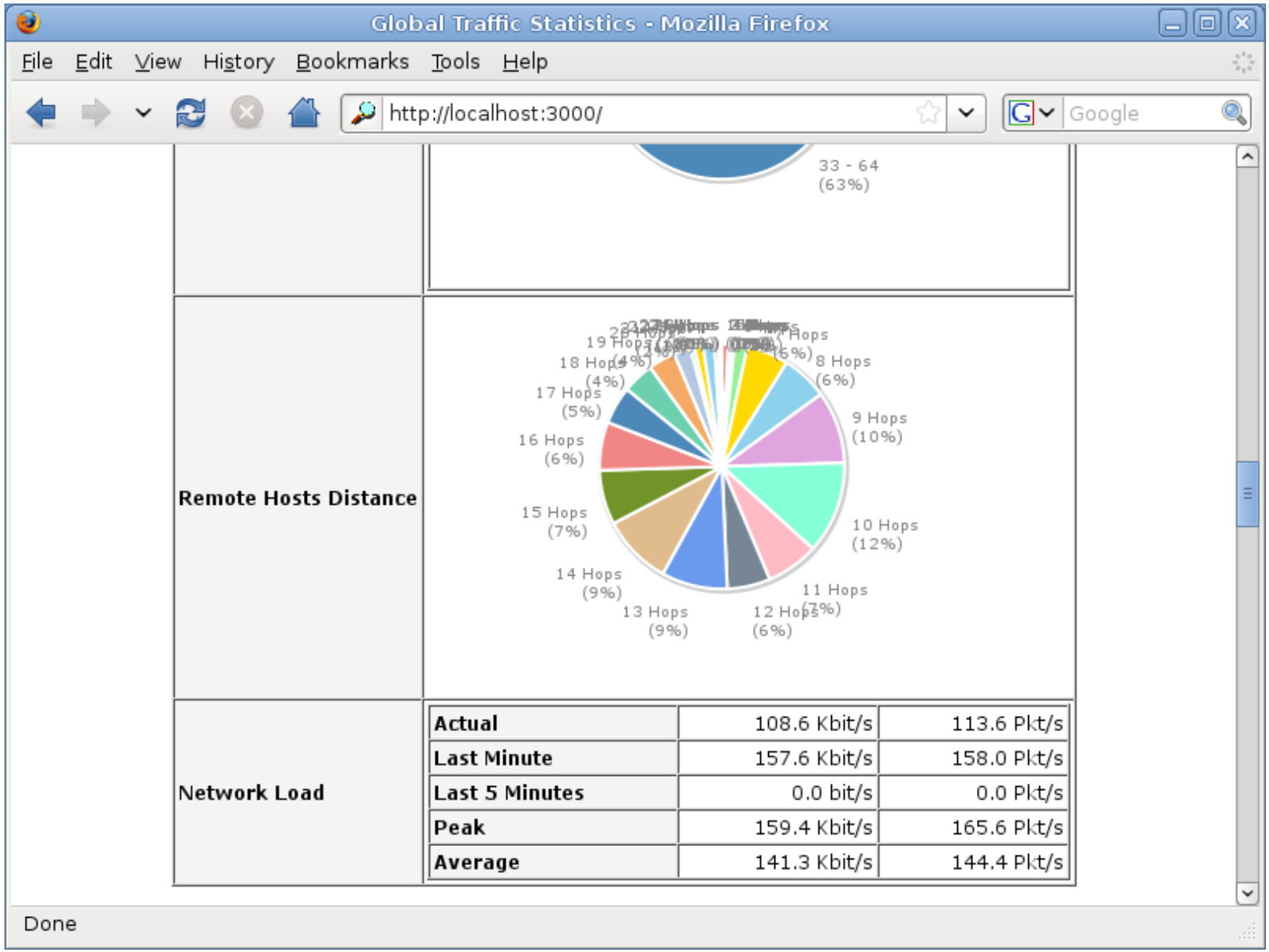
```
> sudo nano /usr/local/nagios/etc/objects/switch.cfg

        define host{
                host_name               router-telecom
                address                 192.168.1.1
                hostgroups              switches
                }
        define service {
           ...
           host_name                    router-telecom
           service_description          PING
           check_command                check_ping!200.0,20%!
        600.0,60%
           check_interval       5
           ...    }
```

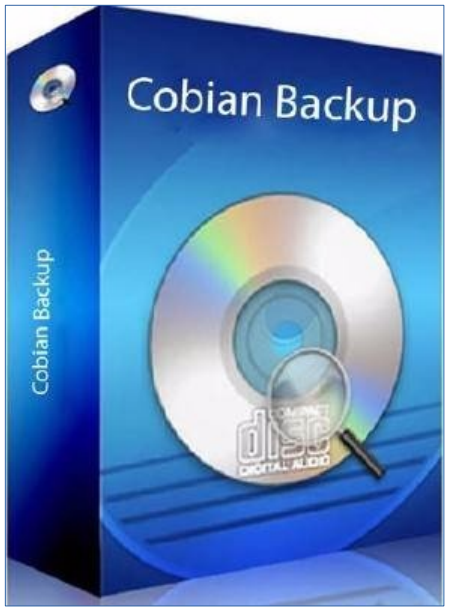
Network monitoring con Nagios®

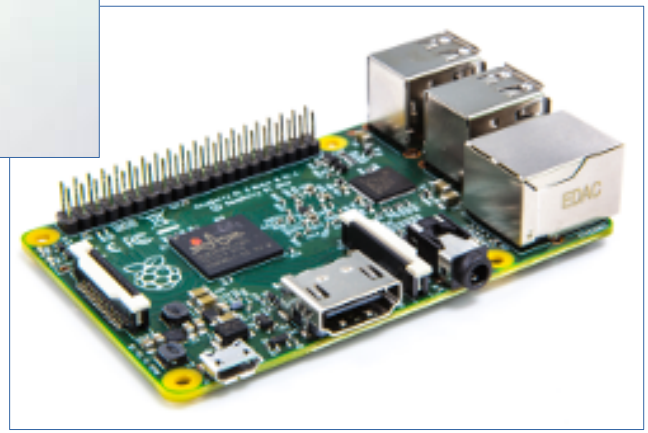


Network monitoring con NTOP



FTP backup a prova di *ransomware*





- L’uso del protocollo FTP rende invisibile la cartella di destinazione dei backup

VSFPTD

Come strumento di pentesting

- Sara' sufficiente un file di SHELL con pochi comandi, da schedulare con CRON

```
> sudo nano /home/pi/pentest.sh

#!/bin/bash
clear
a=$(wget http://ipinfo.io/ip -qO -)
wget
"http://www.marcellini.org/marcellinux/leggimi.php
?myip=$a&ID=1"
rm -f leggimi*
```

- Attraverso CURL si possono postare file in remoto (es. esito di NMAP) o ricevere comandi con WGET

Risultato finale e reali impieghi:

- Monitoraggio dei servizi IT acquistati all'esterno da parte di una compagnia assicurativa;
- Monitoraggio di risorse web che violano il copyright di pezzi esposti presso musei

FINE