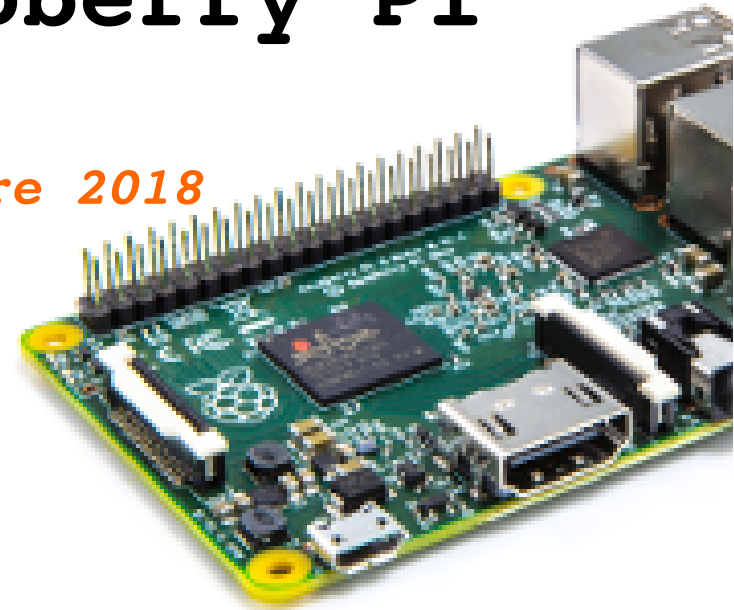




# Monitoraggio e penetration testing di reti LAN con Raspberry Pi

Marco Marcellini – 9 ottobre 2018



MESE

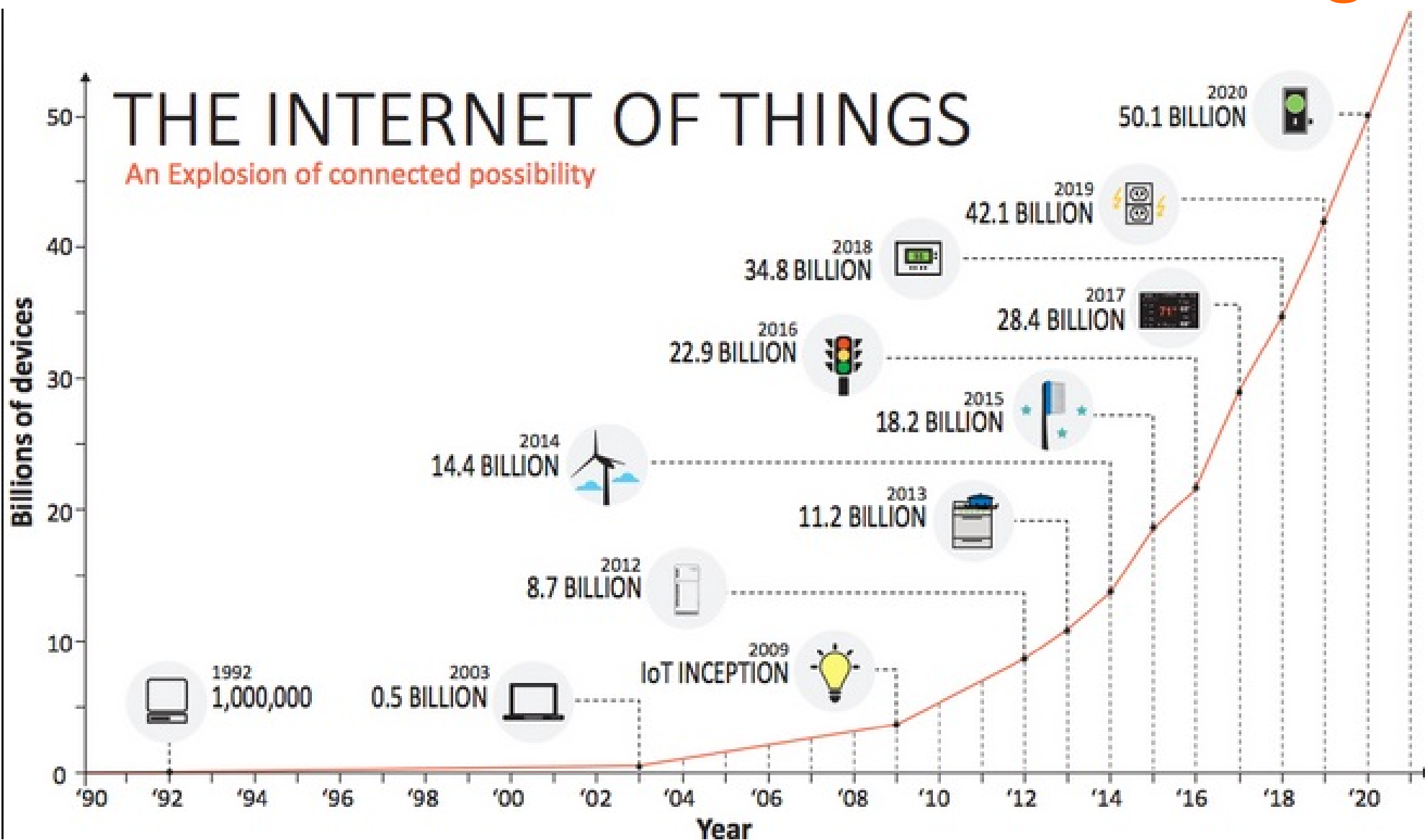
EUROPEO

DELLA

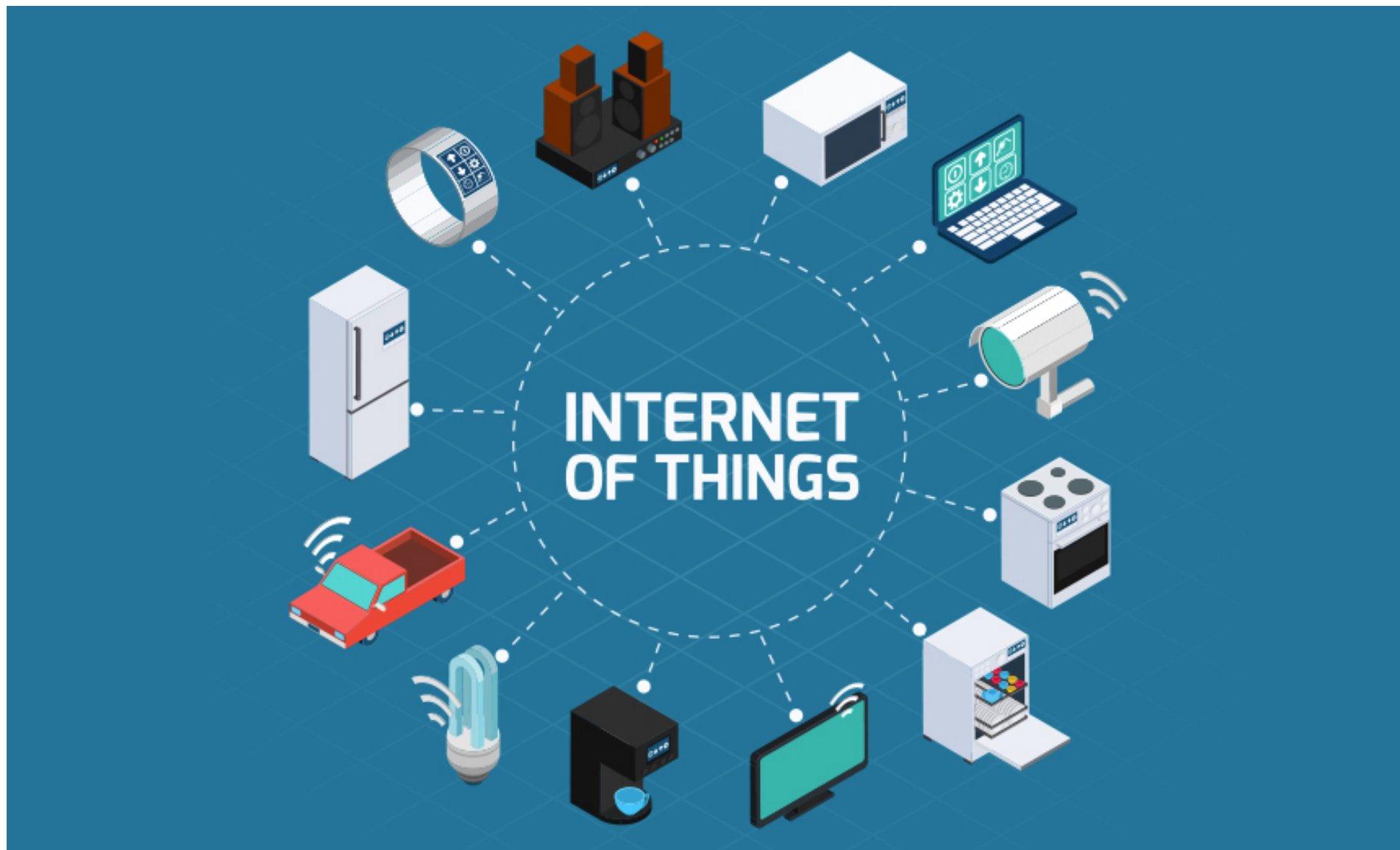
SICUREZZA

INFORMATICA

# Evoluzione dell'Internet of Things

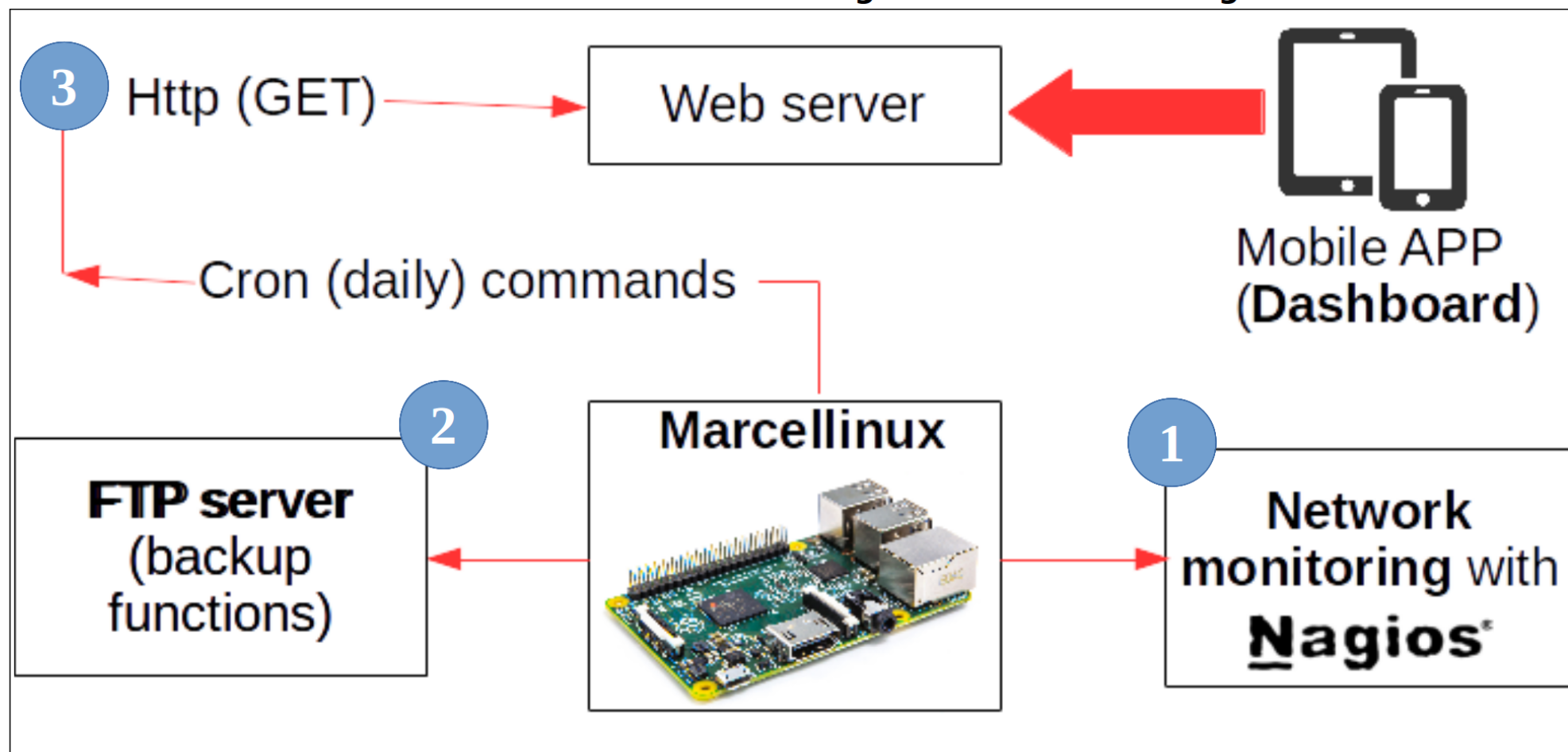


# IoT changes the Cybersecurity Landscape



# L'architettura di *Marcellinux*

Figura 6 - Architettura generale del sistema





# Network monitoring con Nagios®

- Una volta installato Nagios4 dal codice sorgente, sarà 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®

**Nagios®**

**General**

- Home
- Documentation

**Current Status**

- Tactical Overview
- Map (Legacy)
- Hosts
- Services
- Host Groups
  - Summary
  - Grid
- Service Groups
  - Summary
  - Grid
- Problems
  - Services (Unhandled)
  - Hosts (Unhandled)
  - Network Outages

Quick Search:

**Reports**

- Availability
- Trends (Legacy)
- Alerts
  - History
  - Summary
  - Histogram (Legacy)
- Notifications

**Tactical Monitoring Overview**  
 Last Updated: Sat Jun 16 00:46:26 CEST 2018  
 Updated every 90 seconds  
 Nagios® Core™ 4.3.2 - www.nagios.org  
 Logged in as nagiosadmin

**Monitoring Performance**

Service Check Execution Time:	0.01 / 4.16 / 0.945 sec
Service Check Latency:	0.00 / 0.00 / 0.001 sec
Host Check Execution Time:	0.09 / 30.04 / 4.726 sec
Host Check Latency:	0.00 / 0.00 / 0.000 sec
# Active Host / Service Checks:	10 / 9
# Passive Host / Service Checks:	0 / 0

**Network Outages**

0 Outages

**Network Health**

Host Health:

Service Health:

**Hosts**

1 Down      0 Unreachable      9 Up      0 Pending

1 Unhandled Problems

**Services**

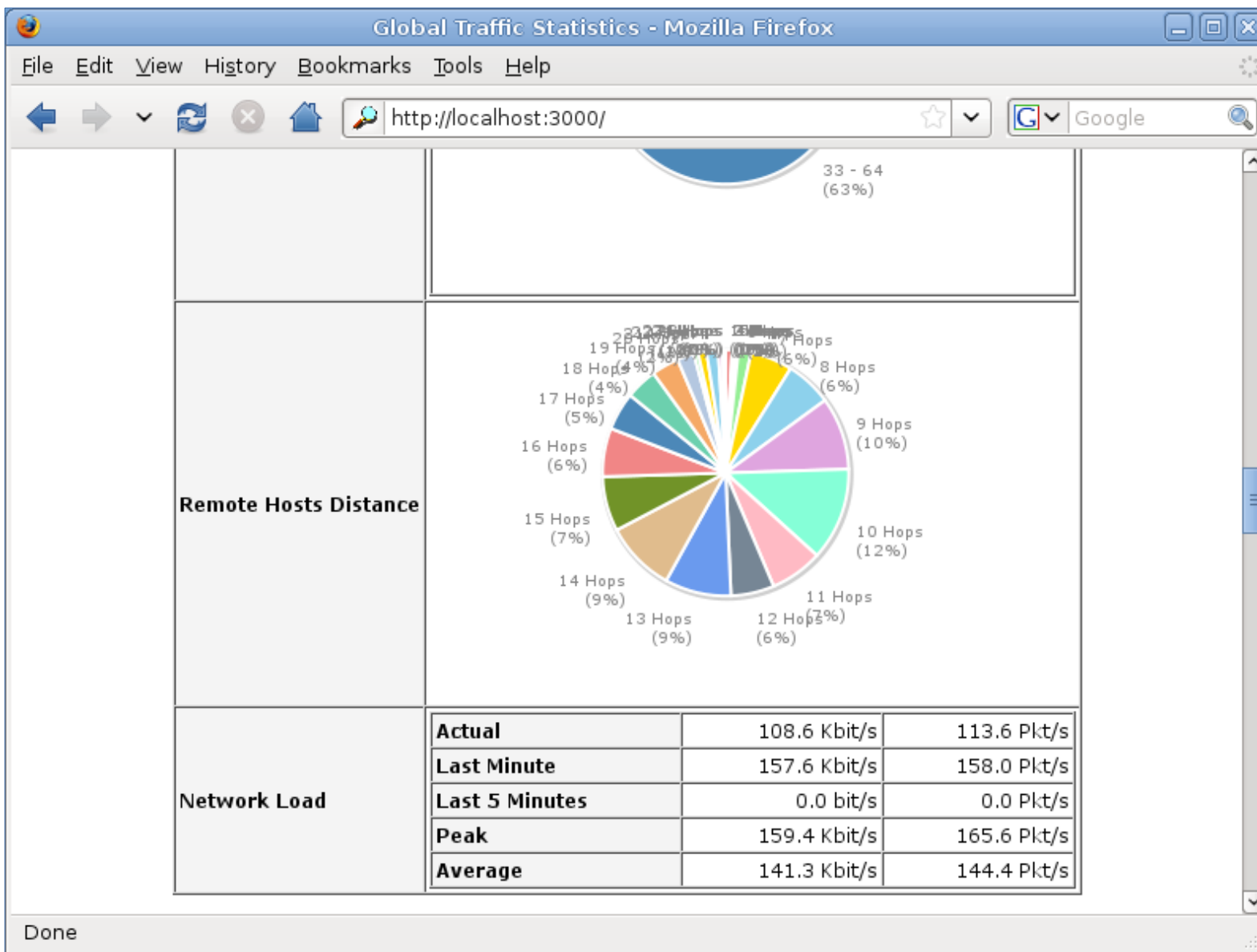
0 Critical      0 Warning      0 Unknown      9 Ok      0 Pending

**Monitoring Features**

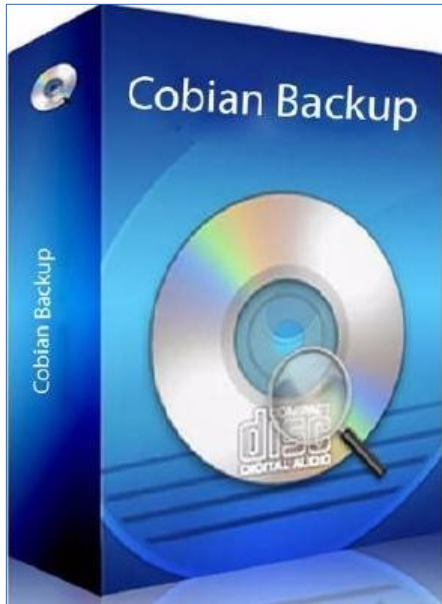
Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks
✓ All Services Enabled	✓ 2 Services Disabled	✓ All Services Enabled	✓ All Services Enabled	✓ All Services Enabled
No Services Flapping	All Hosts Enabled	All Hosts Enabled	All Hosts Enabled	All Hosts Enabled
All Hosts Enabled				



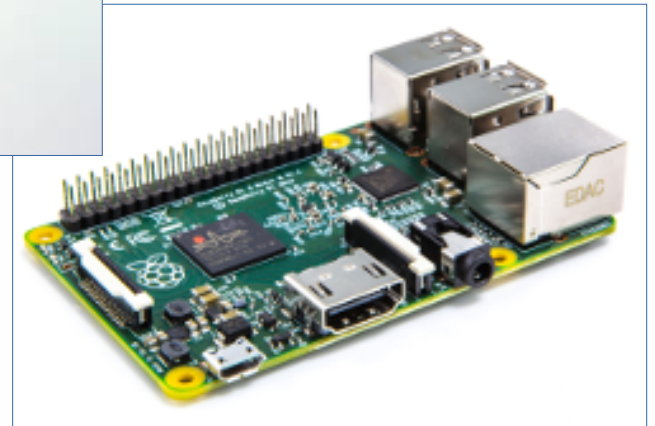
# Network monitoring con NTOP



# FTP backup a prova di *ransomware*



**RANSOMWARE**



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

**VSFPTD**





MESE

EUROPEO

DELLA

SICUREZZA

INFORMATICA

# 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