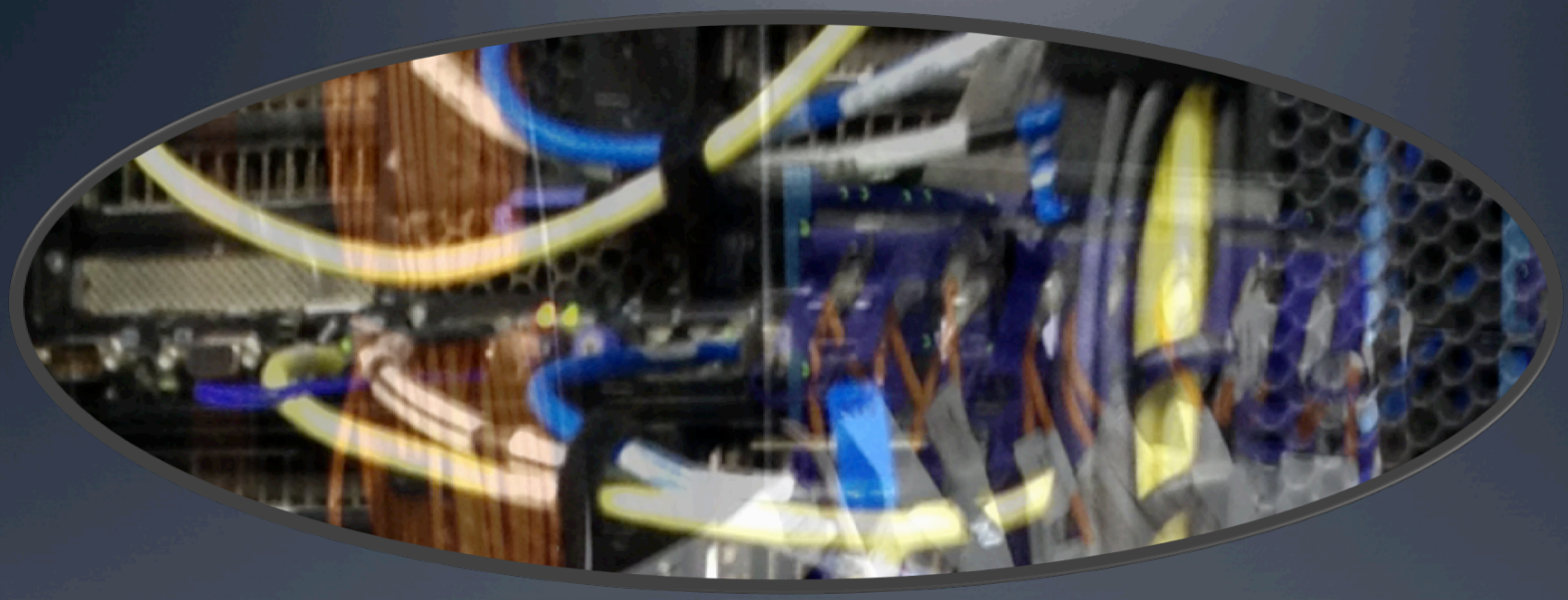


Open Day DFA 2014

Incident Response aziendale

Il DDOS su NTP del 10/2/2014

come l'ho identificato e come ho risposto

Marco Carlo Spada
m.c.spada@mash.it

Marco Carlo Spada

Open Day DFA 2014 – Il DDOS su NTP del 10/2/2014

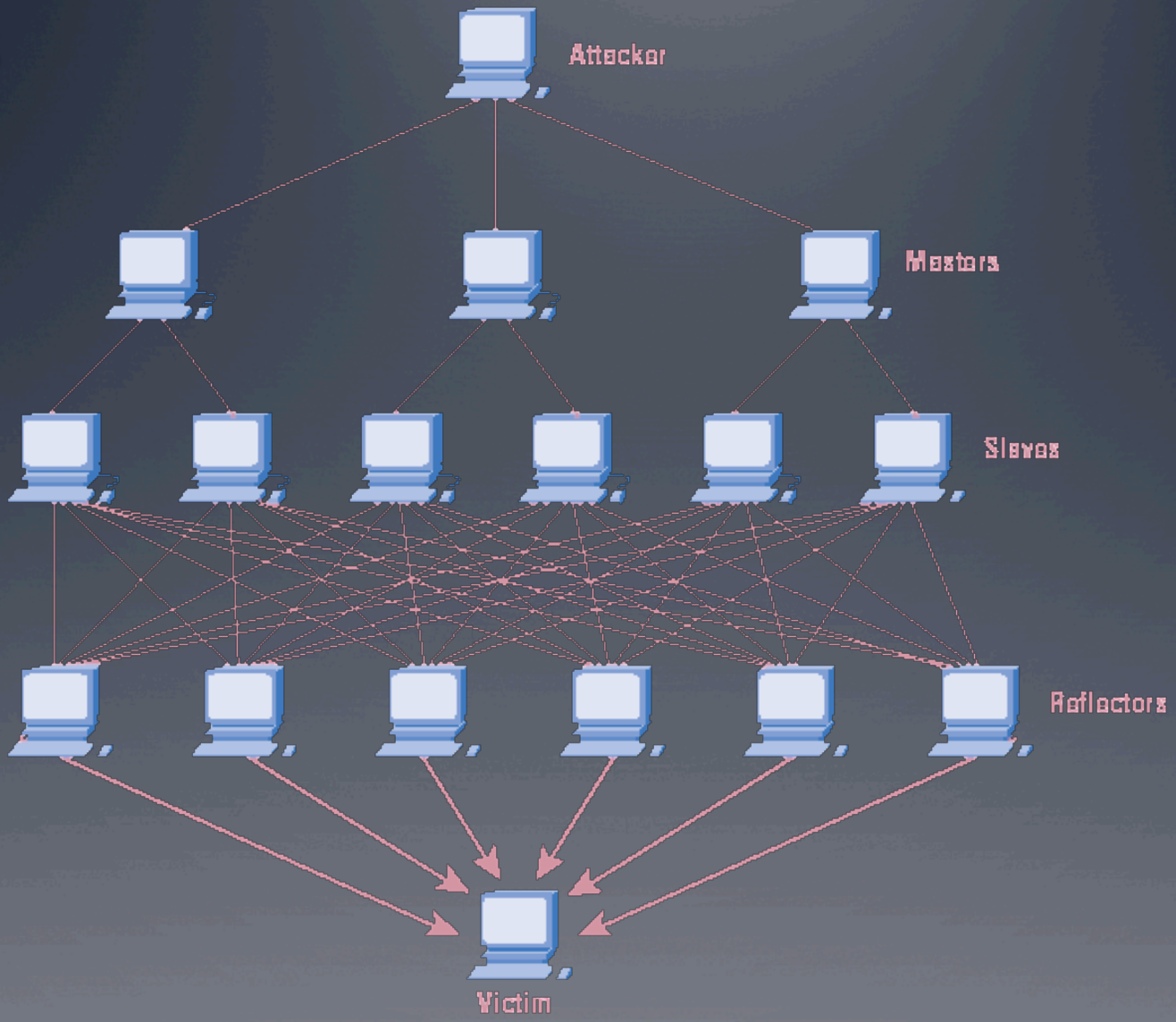

ictB
Home
Ti trovi in:
Attacco D
di Elena Re Ga
pubblicato merc
Cloud Flare ri
potenza deva
anche ai prov
Lunedì è stato
Gbit/s, super
L'attacco è sta
Matthew Princ
registrato lo
Prince ha amm
rifiutato di div
sempre media
spropositata d
ARBOR NETWORKS REGISTRA UN PICCO SENZA PRECEDENTI DELLE DIMENSIONI DEGLI ATTACCHI DDOS VIA NTP
Canale
pubblic
da:
Arbor
DDoS
pubblic
propria
picco
degli at
NTP è
orologi
anche
attacco
indirizz
control
implem
apprez
amplifi
reperib
semplic
ATLAS
condivi
visione
ATLAS
Digital
attacch
FLASH NEWS: ICT: - 4,4% nel 2013
• TTG: nuova puntata
• Software illegali molto costosi
BitMat » Internet
ATTA
Leggi più
Nel prim
periodo
lanciato
L'innova
maggior
nel prim
utilizzar
criminal
protocol
la Repubblica.it
Tom's Hardware è partner del Gruppo Editoriale L'Espresso
KataWeb
L'Espresso
Hardware
Mobile
Videogiochi
Sicurezza
IT Pro
Manager
Reseller
Recupero Dati
Forum
Video
Blog
Shopping
tom's HARDWARE
IT PRO by DIRECTION
Cerca...
IT Pro
Cloud Computing
Communication
ICT Security
Networking
Software
Storage e Server
Kroll Ontrack.
Hai perso i dati?
Sconti esclusivi per i lettori di Tom's
Ti trovi in:
Home Page
IT Pro
ICT Security
Gli attacchi DDoS via NTP crescono in numero e dimensioni
0 COMMENTI
di Riccardo Florio, 13 maggio, 2014 12:20
Lo segnala Arbor Networks che ha calcolato che nel primo trimestre 2014 sono stati registrati 72 attacchi superiori a 100 GB/sec
Mi piace 3
Pin it
Share 0
0
Share 1
NTP è un protocollo basato su UDP utilizzato per sincronizzare orologi attraverso una rete informatica. I servizi basati su UDP includono anche DNS, SNMP, NTP, chargen e RADIUS, che sono quindi potenzialmente vettori di attacco DDoS dal momento che il protocollo è di
nel precedente trimestre fino a raggiungere la stessa percentuale di diffusione degli attacchi SYN flood, una delle tipologie di attacchi DDoS da sempre preferite dai criminali informatici.
Prepare for DDoS Attacks
prolexic.com/ddos-attack-reports
Get the DDoS attack report - Free! Find out what DDoSers are doing now
DDoS Testing Service
Trasforma vasca in doccia

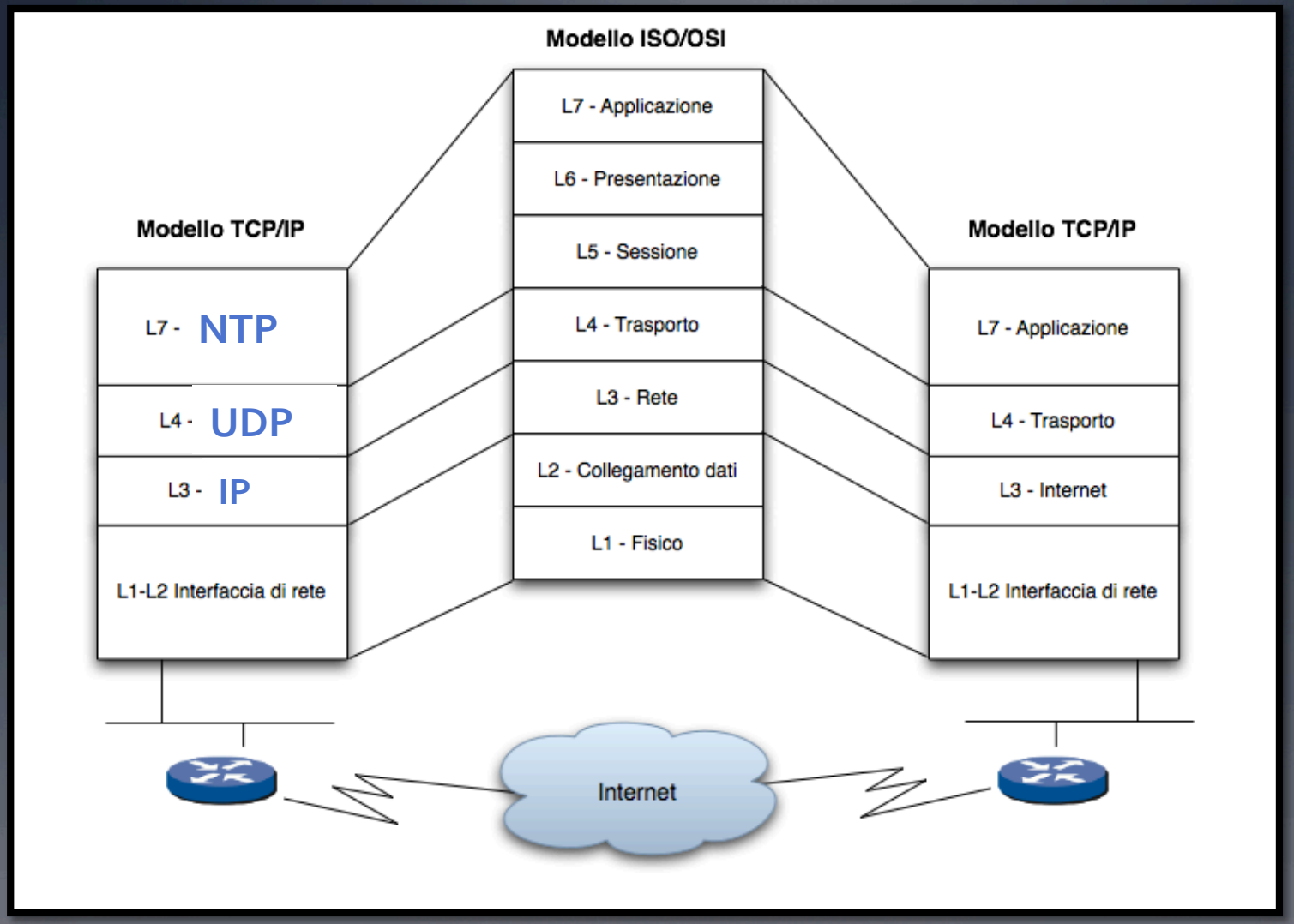
PAROLE CHIAVE:

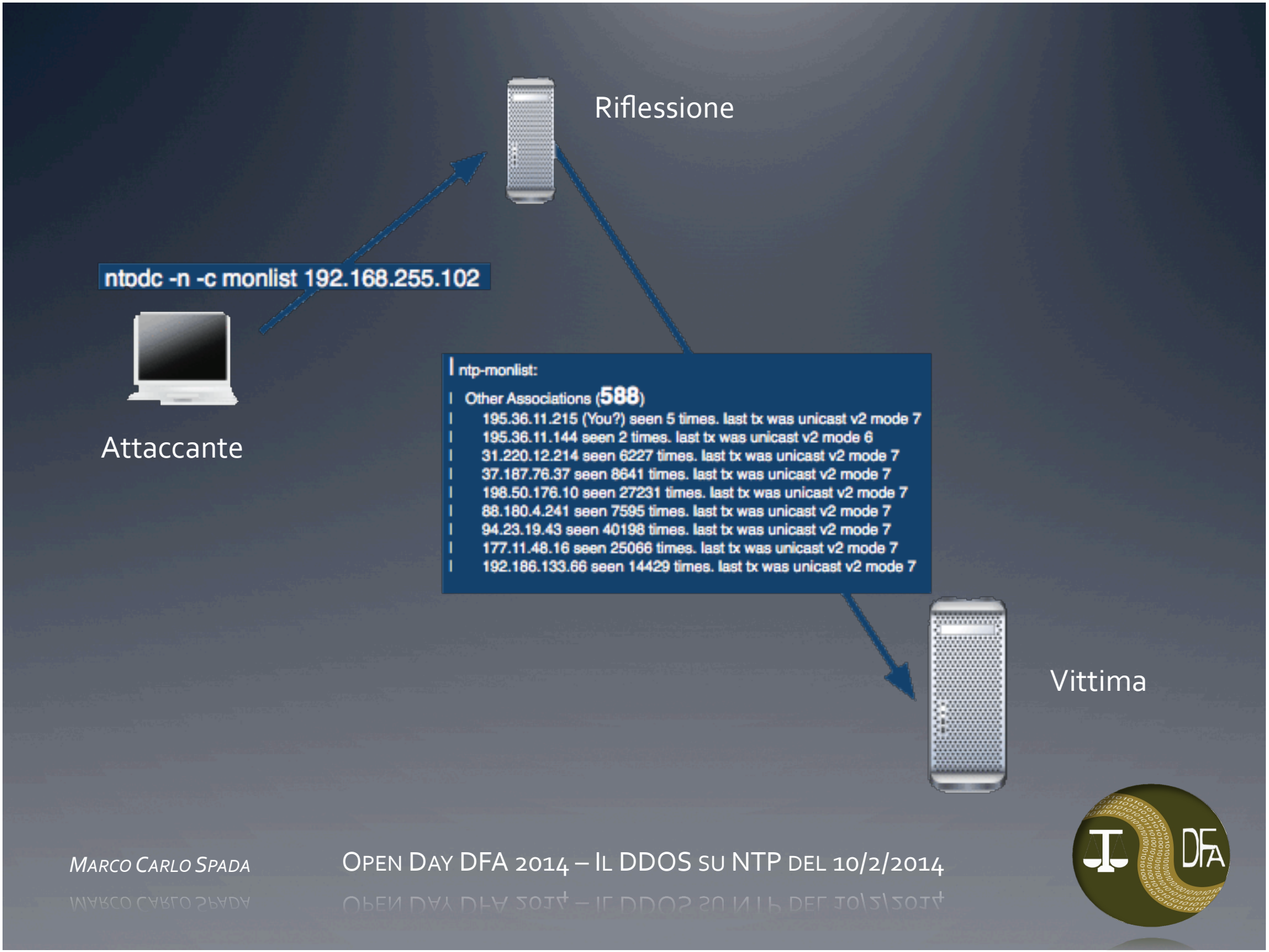
- DDOS
- NTP
- REFLECTION

- MRTG
- tcpdump
- nmap

- DDOS

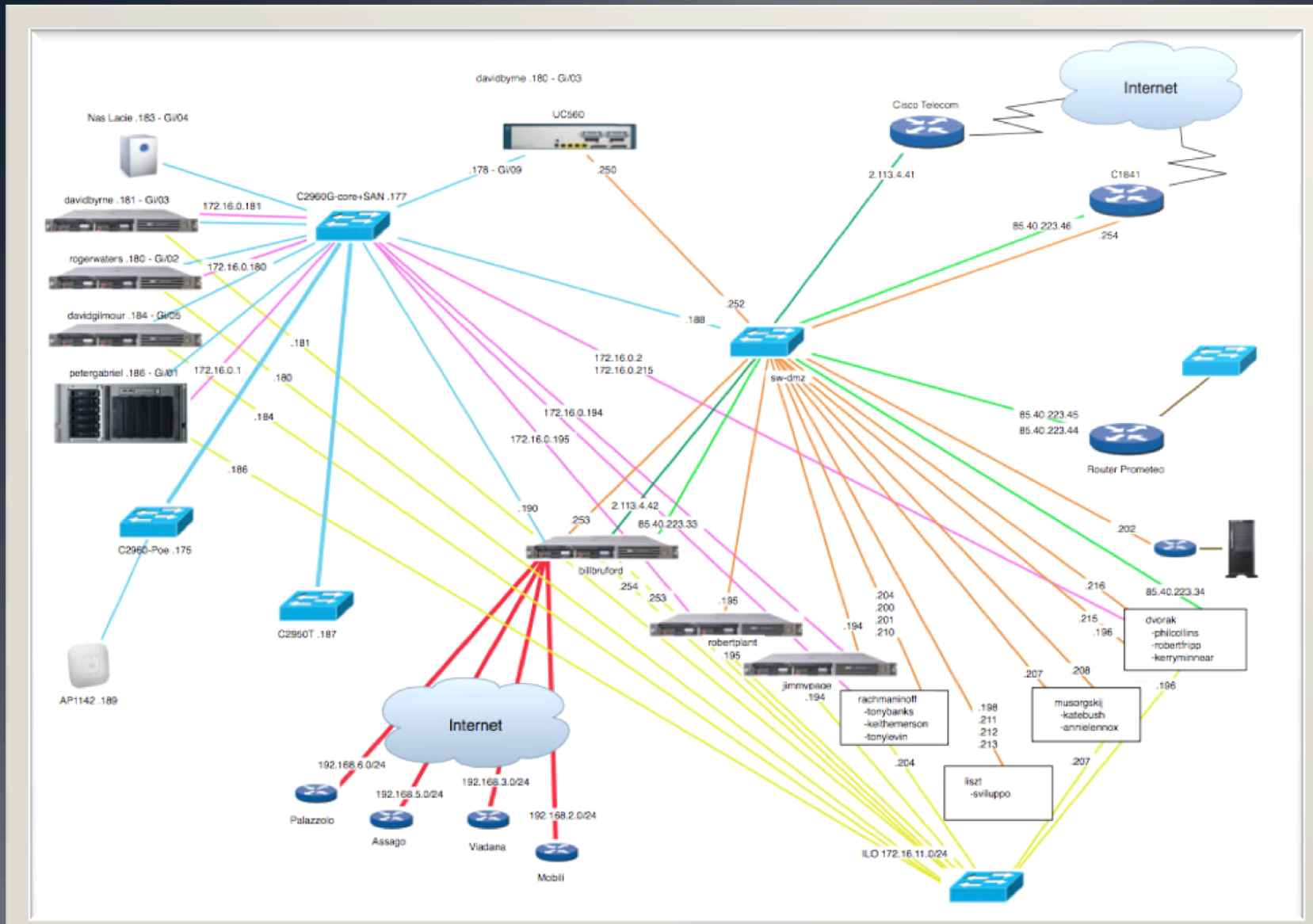



Modello ISO/OSI
L7 - Applicazione
L6 - Presentazione
L5 - Sessione
L4 - Trasporto
L3 - Rete
L2 - Collegamento dati
L1 - Fisico
Modello TCP/IP
L7 - NTP
L4 - UDP
L3 - IP
L1-L2 Interfaccia di rete
Modello TCP/IP
L7 - Applicazione
L4 - Trasporto
L3 - Internet
L1-L2 Interfaccia di rete
Internet


Riflessione
ntpdc -n -c monlist 192.168.255.102
Attaccante
ntp-monlist:
Other Associations (588)
195.36.11.215 (You?) seen 5 times. last tx was unicast v2 mode 7
195.36.11.144 seen 2 times. last tx was unicast v2 mode 6
31.220.12.214 seen 6227 times. last tx was unicast v2 mode 7
37.187.76.37 seen 8641 times. last tx was unicast v2 mode 7
198.50.176.10 seen 27231 times. last tx was unicast v2 mode 7
88.180.4.241 seen 7595 times. last tx was unicast v2 mode 7
94.23.19.43 seen 40198 times. last tx was unicast v2 mode 7
177.11.48.16 seen 25066 times. last tx was unicast v2 mode 7
192.186.133.66 seen 14429 times. last tx was unicast v2 mode 7
Vittima

Fattori di amplificazione di alcuni protocolli applicazione su UDP

DNS	da 28 a 54
NTP	556.9
SNMPv2	6.3
NetBIOS	3.8
SSDP	30.8
CharGEN	358.8
QOTD	140.3
BitTorrent	3.8

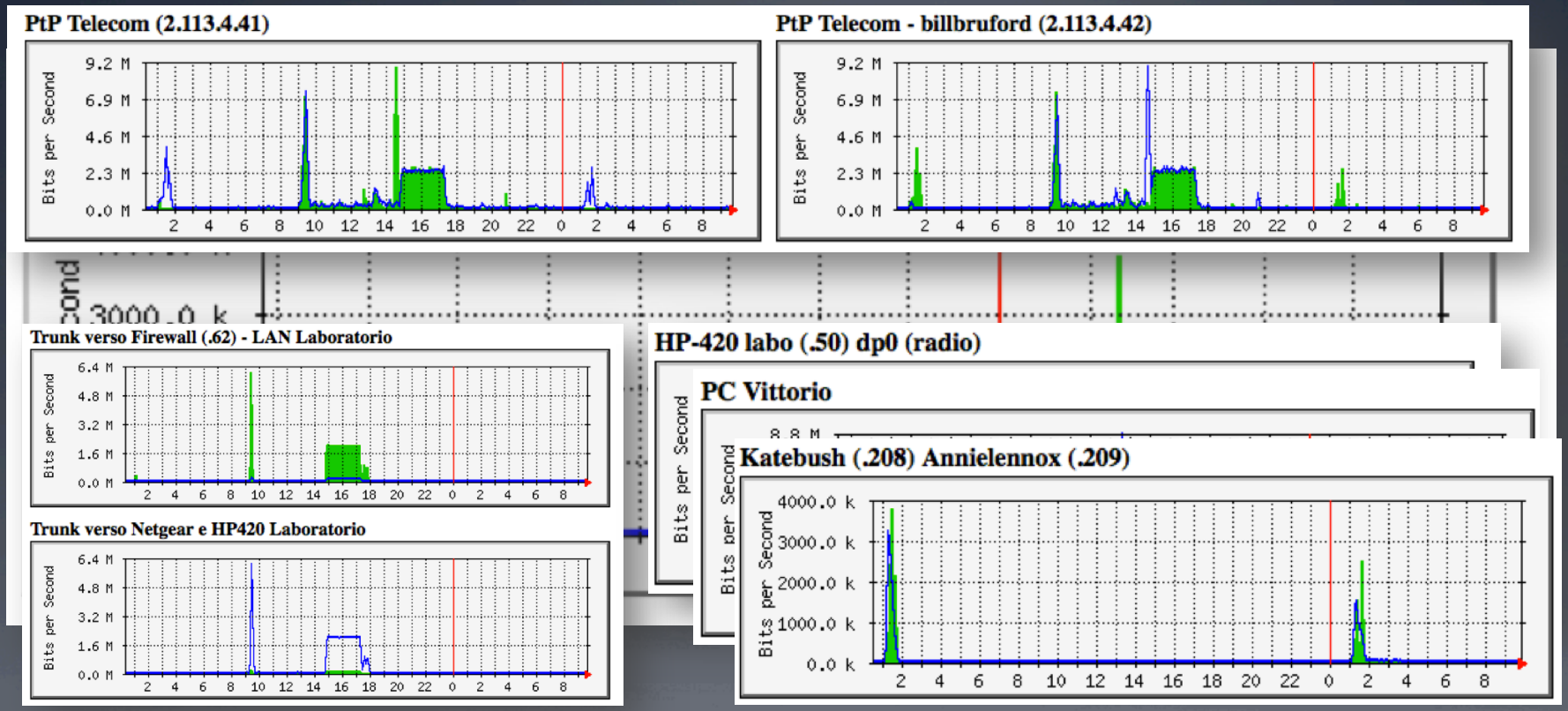

Internet
Cisco Telecom
2.113.4.41
C1841
85.40.223.46
.254
UC560
.178 - Gi/09
.250
davidbyrne .180 - Gi/03
Nas Lacie .183 - Gi/04
davidbyrne .181 - Gi/03
172.16.0.181
C2960G-core+SAN .177
rogerwaters .180 - Gi/02
172.16.0.180
davidgilmour .184 - Gi/05
petergabriel .186 - Gi/01
172.16.0.1
.180
.181
.184
.186
.188
.252
172.16.0.2
172.16.0.215
sw-dmz
172.16.0.194
172.16.0.195
85.40.223.45
85.40.223.44
Router Prometeo
.202
.216
85.40.223.34
dvorak
-philcollins
-robertfripp
-kerryminnear
.215
.196
.207
.208
.196
musorgskij
-katebush
-annielennox
.198
.211
.212
.213
.204
.207
liszt
-sviluppo
ILO 172.16.11.0/24
.190
.253
2.113.4.42
85.40.223.33
billbruford
.254
.253
.195
robertplant
.195
.204
.200
.201
.210
.194
jimmypage
.194
rachmaninoff
-tonybanks
-keithemerson
-tonylevin
C2960-Poe .175
C2950T .187
AP1142 .189
Internet
192.168.6.0/24
192.168.5.0/24
192.168.3.0/24
192.168.2.0/24
Palazzolo
Assago
Viadana
Mobili

Tassonomia dei monitoraggi di rete

K. J. Jones, R. Bejtlich e C. W. Rose
Real Digital Forensics, Computer Security and Incident Response

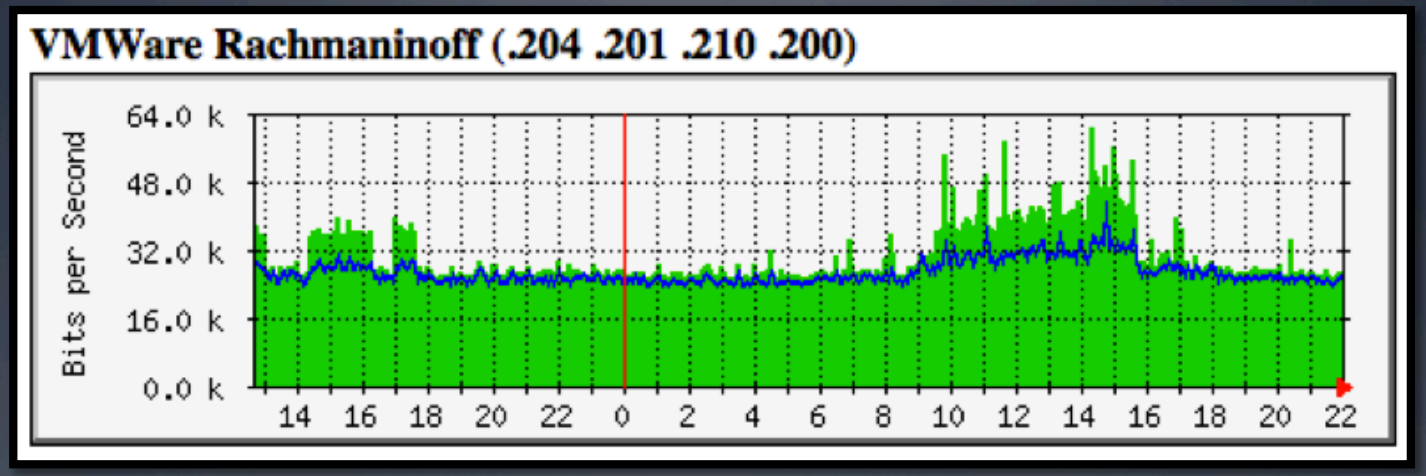
- Full content data
- Session data
- Alert data
- Statistical data

MRTG: esempi di anomalie

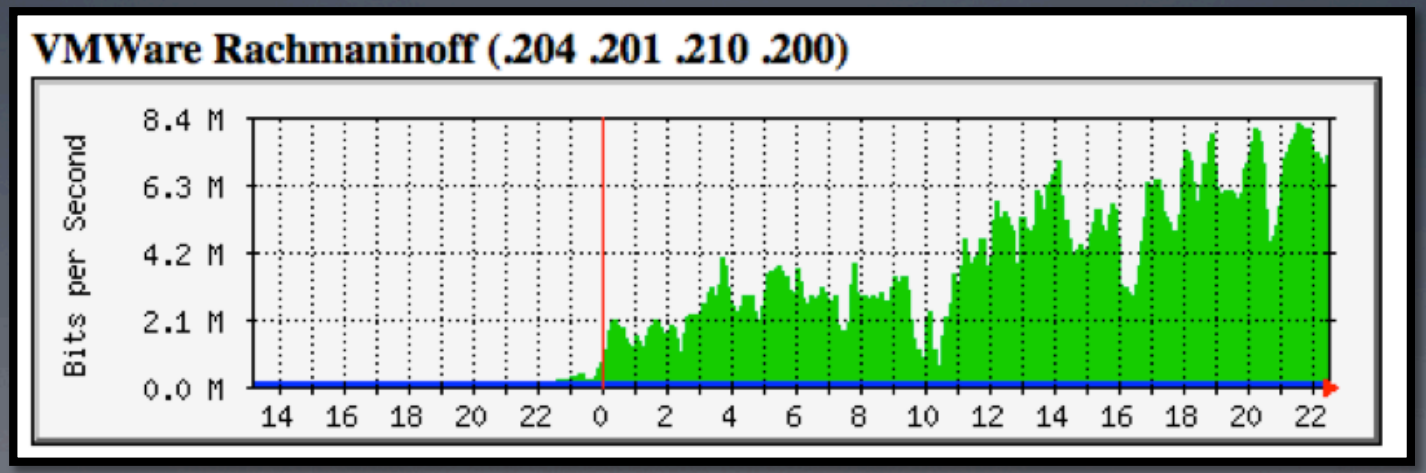


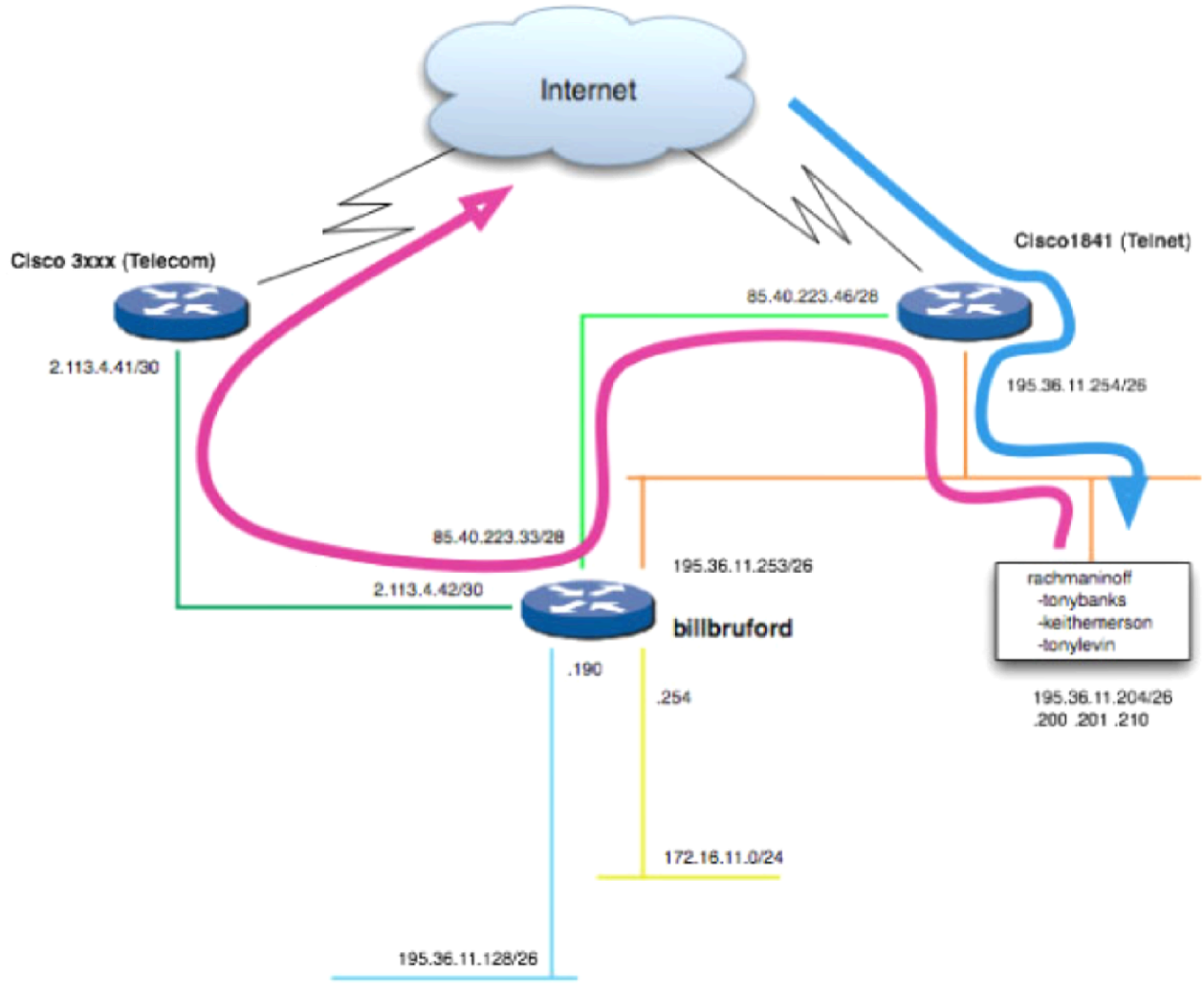
MRTG: switch DMZ porta Fa 0/12

normale



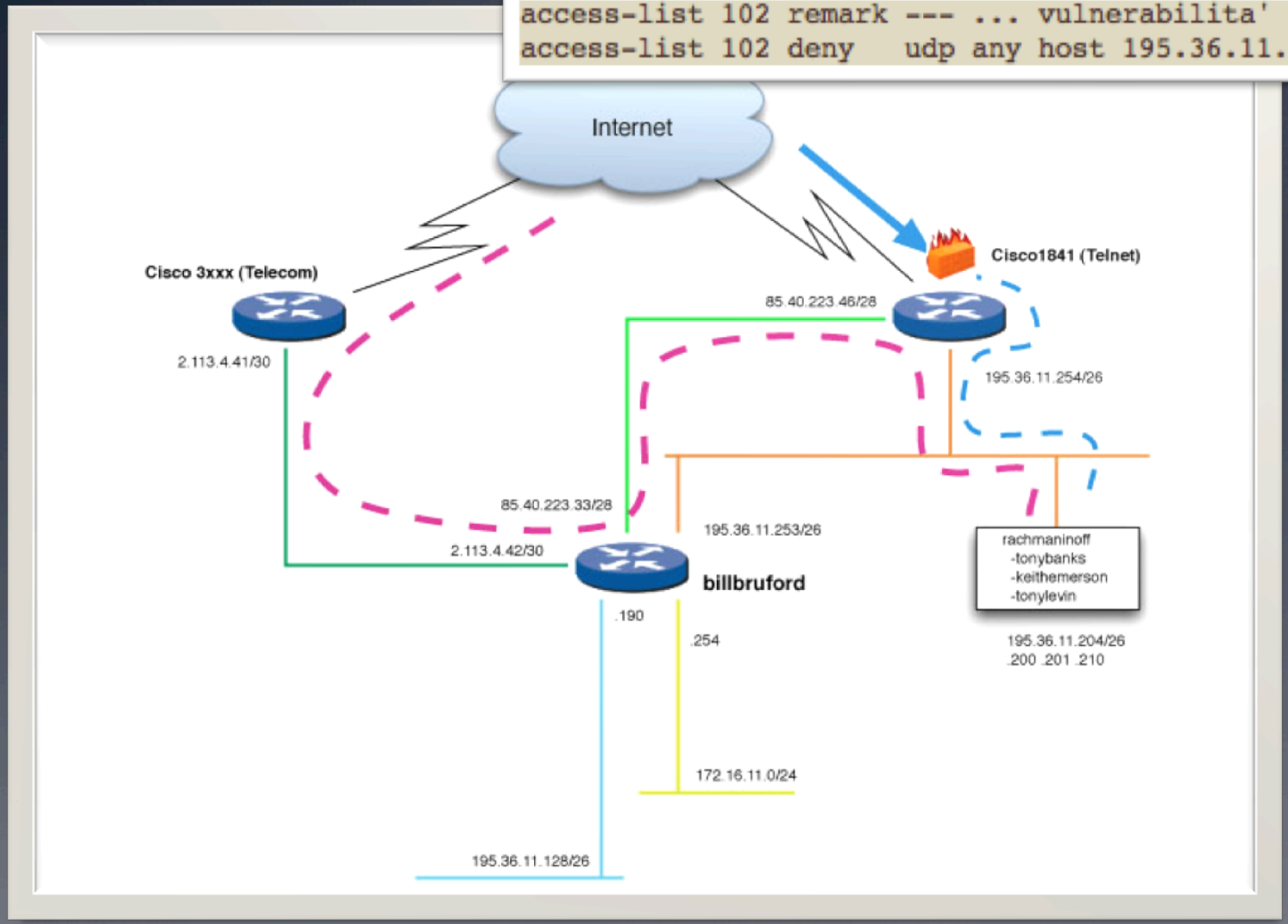
10/2/2014




Internet
Cisco 3xxx (Telecom)
2.113.4.41/30
85.40.223.46/28
Cisco1841 (Telnet)
195.36.11.254/26
85.40.223.33/28
195.36.11.253/26
2.113.4.42/30
billbruford
.190
.254
rachmaninoff
-tonybanks
-keithemerson
-tonylevin
195.36.11.204/26
.200 .201 .210
172.16.11.0/24
195.36.11.128/26

Soluzione: ACL sul cisco!

```
access-list 102 remark --- ... vulnerabilita' udp su VMWare
access-list 102 deny   udp any host 195.36.11.204
```



Ho finito?

1. Analisi dei dati raccolti e approfondimenti:
   studio del tipo di attacco e dei precedenti noti,
   delle vulnerabilità segnalate e dei bollettini.

2. Verifica estesa su tutte le altre reti/installazioni,
   aggiornamento degli strumenti di indagine (nmap).

3. Riesame critico dell'implementazione per individuare eventuali interventi migliorativi sull' infrastruttura, eventualmente da tener in conto nella progettazione delle prossime realizzazioni.

Marco Carlo Spada
m.c.spada@mash.it

Open Day DFA 2014 – Il DDOS su NTP del 10/2/2014