Aspetti tecnici della sicurezza nei servizi

- Considerazioni legali: privacy e trattamento dati giudiziari, sensibili e personali, decreto antiterrorismo, decreti del garante
- Firewall perimetrale
- Servizi:
  - Certification Authority
  - Mail (Pec, antivirus, antispam)
  - DNS (Politiche: indirizzi pubblici e privati e sicurezza passiva)
  - Accesso wireless (TRIP)
  - VPN
  - Web
  - IDS (NTOP)
  - Auditing (Sicurezza e versioni di sistemi operativi e prodotti)

Considerazioni legali - 1

Nel 2002 l'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) ha prodotto delle linee guida per la sicurezza informatica negli Enti pubblici dei Paesi membri.

L'Italia si è data una Direttiva del Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri (2002) per stabilire linee di condotta per la sicurezza dei sistemi informatici con riguardo anche ai dati personali e sensibili.

Considerazioni legali - 2

L'INFN – attraverso un apposito gruppo di lavoro - ha prodotto la documentazione indicata dal Dipartimento per l'Innovazione, nella forma di:

- **Carta della sicurezza** diretta a definire obiettivi e finalità delle politiche di sicurezza, le strategie di sicurezza, il modello organizzativo ed i processi per attuarle;

- **Politiche generali di sicurezza**, che le direttive generali per lo sviluppo, gestione, controllo e verifica delle misure da adottare;

- **Politiche specifiche di sicurezza (Norme)** costituite da un **Regolamento per l'uso delle risorse informatiche dell'INFN.**

Considerazioni legali – 3

Disposizioni in materia di custodia e gestione di archivi di dati personali e sensibili.

- Il Decreto del Presidente della Repubblica (DPR) n. 318/1999
- Il Decreto Legislativo (D. Lgs.) n. 196/2003
- Il Decreto del Garante della Privacy 27/11/08

Questa legislazione impone a tutti gli Enti pubblici di produrre annualmente un **Documento Programmatico sulla Sicurezza Informatica (DPS).**

Considerazioni legali - 4

Documento Programmatico sulla Sicurezza
Anno 2007

1. Introduzione

Il contenuto del Documento Programmatico sulla Sicurezza è indicato al punto 19 dell'Allegato B al Decreto legislativo 30 giugno 2003 n. 196 - Codice in materia di protezione dei dati personali, il quale dispone:

Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

1. *l'elenco dei trattamenti di dati personali;*
2. *la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;*
3. *l'analisi dei rischi che incombono sui dati;*
4. *le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;*
5. *la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;*
6. *la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;*
7. *la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;*
8. *per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.*

Considerazioni legali - 5

	Accesso non autorizzato	Malware	Denial of Service	Furto	Manomissione	Uso non autorizzato
S. O. Windows	M	M	B	B	B	B
S. O. VMS	M	B	B	B	B	M
S. O. Sun Solaris	B	B	B	B	B	B
SW Amministrazione (VMS)	M	B	B	B	B	M

6

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (ANNO 2010)

	Accesso non autorizzato	Malware	Denial of Service	Furto	Manomissione	Uso non autorizzato
SW Amministrazione (Window	B	M	B	B	B	B

Considerazioni legali – 6

Designazioni degli incaricati alle funzioni di amministratore di sistema

Il sottoscritto, <*Nome e Cognome*>, in qualità di Direttore della <*nome struttura*> e responsabile del trattamento dei dati personali,

DESIGNA

le persone sotto elencate quali **amministratori di sistemi elettronici** impiegati per il trattamento di dati personali, nell'ambito a ciascuno indicato,

CONSEGNA

a ciascun amministratore le istruzioni di condotta, prescrivendone l'osservanza, rinviando, altresì,a quanto prescritto nelle note tecniche disponibili alla pagina web http://www.infn.it/CCR/progetti/documentazione/Harmony_sicurezza.htm

Cognome	Nome	Ambito di trattamento	Conferimento incarico e ricevuta istruzioni di condotta		Revoca Incarico	
			Data	Firma Incaricato	Data	Firma Incaricato
COGNOME	***Nome***	*Descrizione attività*[1]				
COGNOME	***Nome***	*Descrizione attività*[1]				
...						

Il Direttore

Considerazioni legali - 7

Il Decreto interministeriale 16 agosto 2005

- Il decreto interministeriale del 16/8/05 contiene misure antiterrorismo volte all'identificazione degli autori di crimini informatici.
- Fa riferimento ai Service Provider, ma si applica a tutti coloro che forniscono accesso alla rete a terzi.
- Ci riguarda perché diamo accesso alla rete anche a persone non dipendenti dell'Ente.

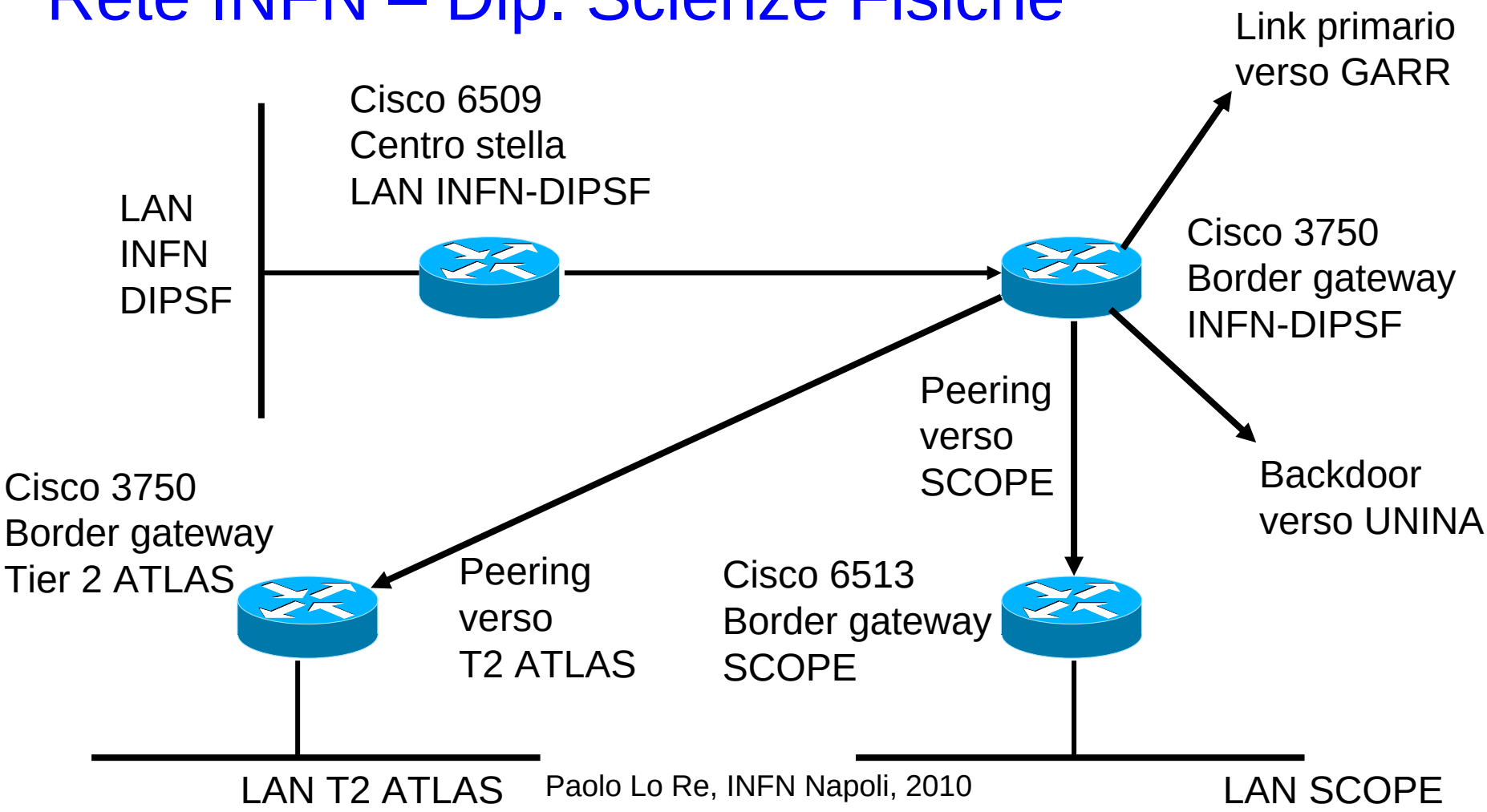
Considerazioni legali - 8

Misure prescritte dal decreto

- Impedire l'accesso alla rete informatica a soggetti non previamente identificati;
- Identificare chi accede mediante acquisizione di dati anagrafici e copia in formato digitale del documento di identità;
- Informare il pubblico delle condizioni d'uso;
- Rendere disponibili i dati acquisiti alla polizia postale, giudiziaria o all'Autorità Giudiziaria (solo quando queste autorità lo richiedano);
- Assicurare il trattamento e la conservazione dei dati fino al 31/12/2007.

Firewall perimetrale - 1

Rete INFN – Dip. Scienze Fisiche



Firewall perimetrale - 2

Il firewall perimetrale della rete INFN-DIPSF è realizzato mediante l'utilizzo di **Access Control List (ACL)** sul router di frontiera.

Le ACL sono linee di comando che vengono eseguite sequenzialmente dal router e permettono di applicare dei filtri sul traffico in transito e sono eseguite sui singoli pacchetti IP.

Firewall perimetrale - 3

Esempio di ACL (Cisco IOS)

```
access-list 101 permit tcp any 192.84.134.0 0.0.0.255 established
access-list 101 permit tcp any 192.84.149.0 0.0.0.255 established
access-list 101 permit tcp any 192.84.156.0 0.0.0.255 established
access-list 101 permit tcp any 192.135.13.0 0.0.0.255 established
access-list 101 permit tcp any 192.135.36.0 0.0.0.255 established
access-list 101 permit tcp any 192.167.203.0 0.0.0.255 established
access-list 101 permit tcp any 193.205.223.0 0.0.0.255 established
!
access-list 101 permit tcp any host 192.135.13.7 eq smtp
access-list 101 permit tcp any host 192.84.134.181 eq smtp
access-list 101 permit tcp any host 192.84.134.182 eq smtp
access-list 101 permit tcp any host 192.84.156.9 eq smtp
access-list 101 deny   tcp any any eq smtp
```

Firewall perimetrale – 4

Esempio di ACL complesse (rate limiting)

```
....

class-map match-all classrv                          <--------- crea la class-map classrv
  description Filtro porte GridFTP                              che si applica alle porte
  match access-group 110                                        specificate dall'access-group 110
!


policy-map policyrv                                  <--------- crea la policy-map policyrv che applica la policy
 description Filtro porte GridFTP a 900MBps                     sotto indicata alla class-map classrv
 class classrv
 police 900000000 1000000 exceed-action drop         <--------- specifica la policy da adottare:
                                                                blocca il traffico superiore a 900 Mbps
                                                                con un massimo di 1 Mbps in più
…

interface GigabitEthernet1/0/3
 description Link -> GARR
 no switchport
 ip address 193.206.130.114 255.255.255.252
 service-policy input policyrv                        <---------- applica la policy policyrv all'interfaccia

....
access-list 110 permit tcp any any range 20000 25000  <------- porte ben note a cui si applica la policy
```

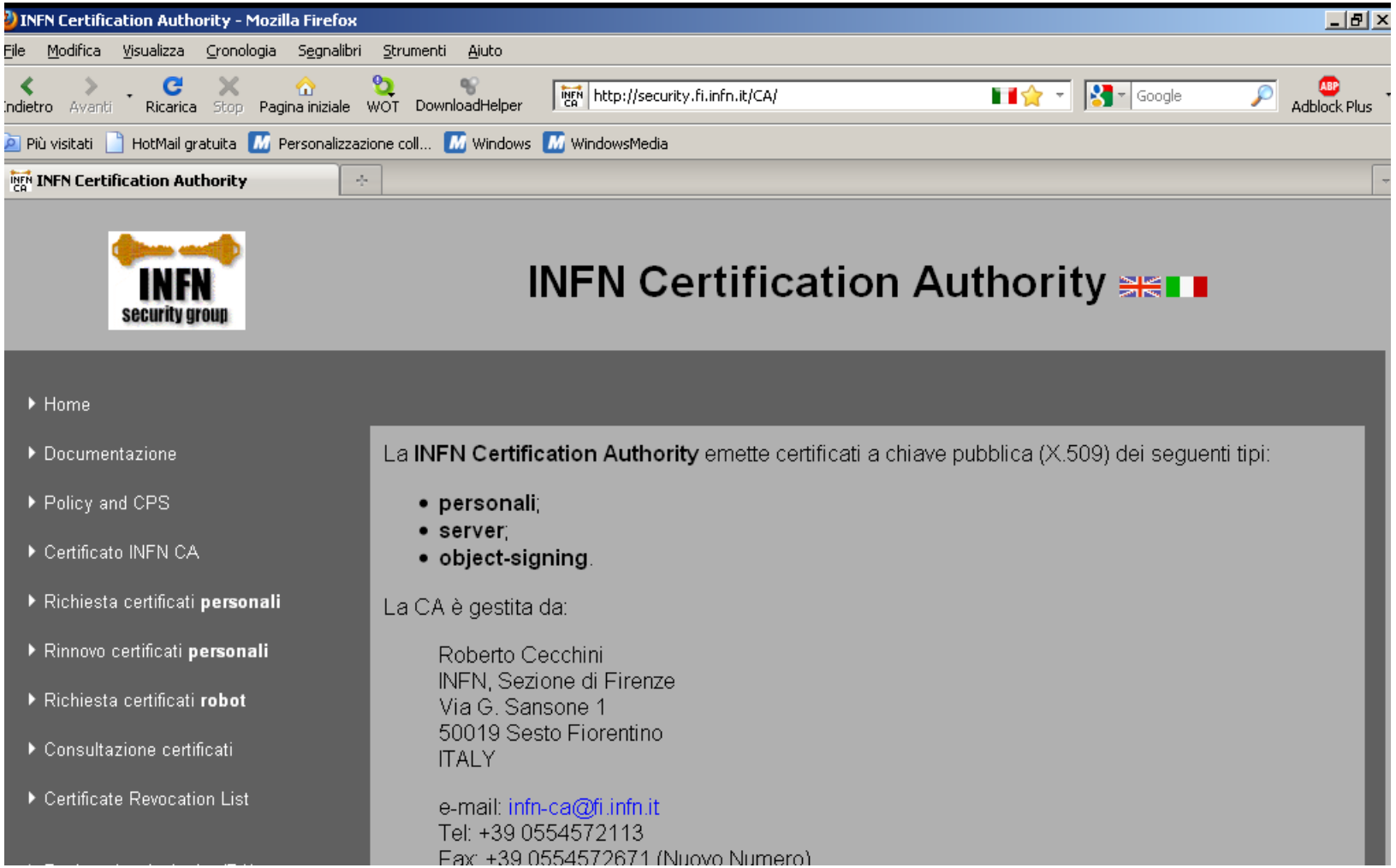
Certification Authority - 1

L'identificazione degli utenti nell'uso delle Griglie Computazionali si basa su certificati elettronici secondo lo standard X509.

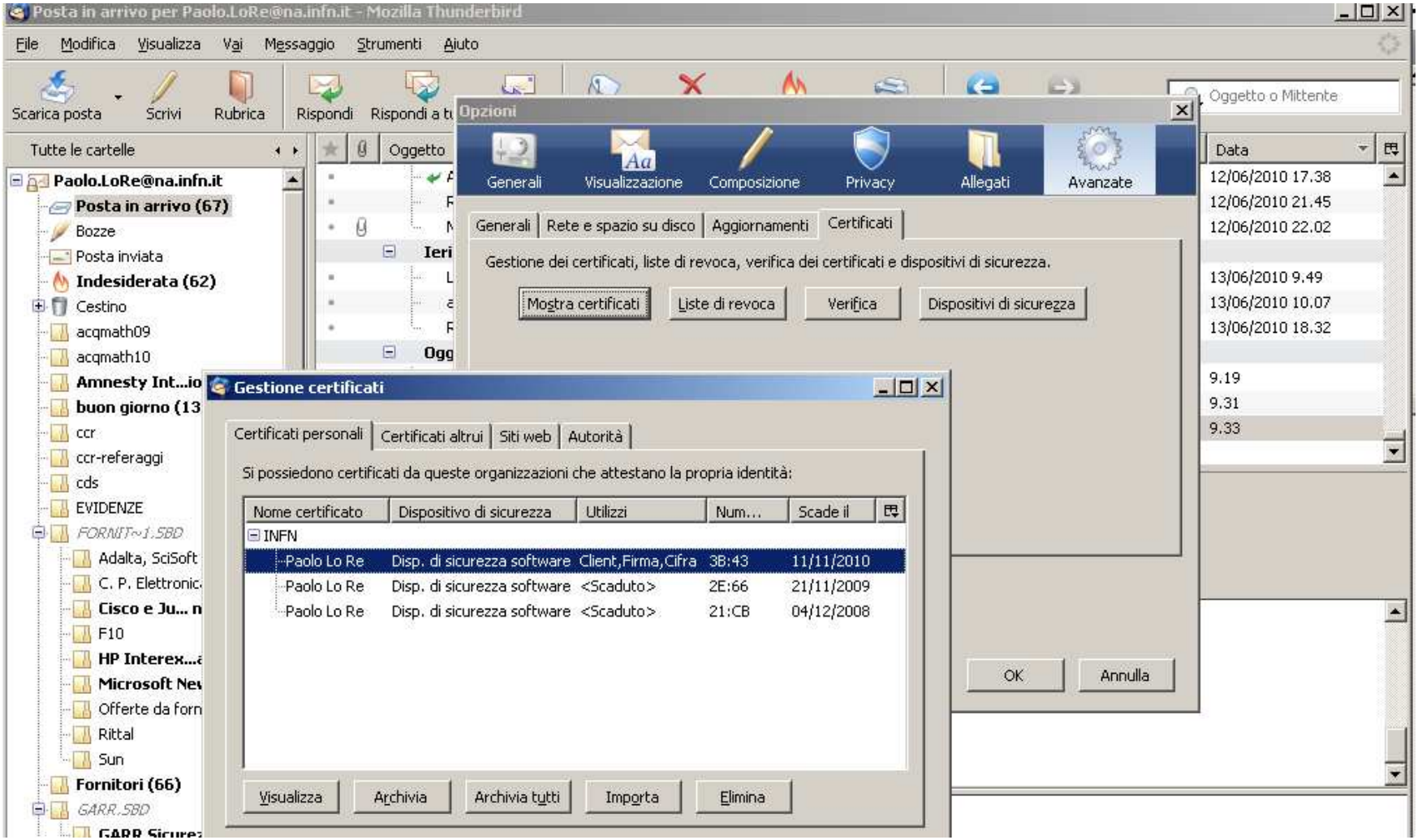
L'INFN si è dotata di una **Certification Authority** che provvede all'emissione dei certificati.

Questi certificati sono usati – in ambito scientifico – anche per l'identificazione degli utenti nell'accesso alla rete wireless e per **posta elettronica certificata (pec).**

Certification Authority - 2

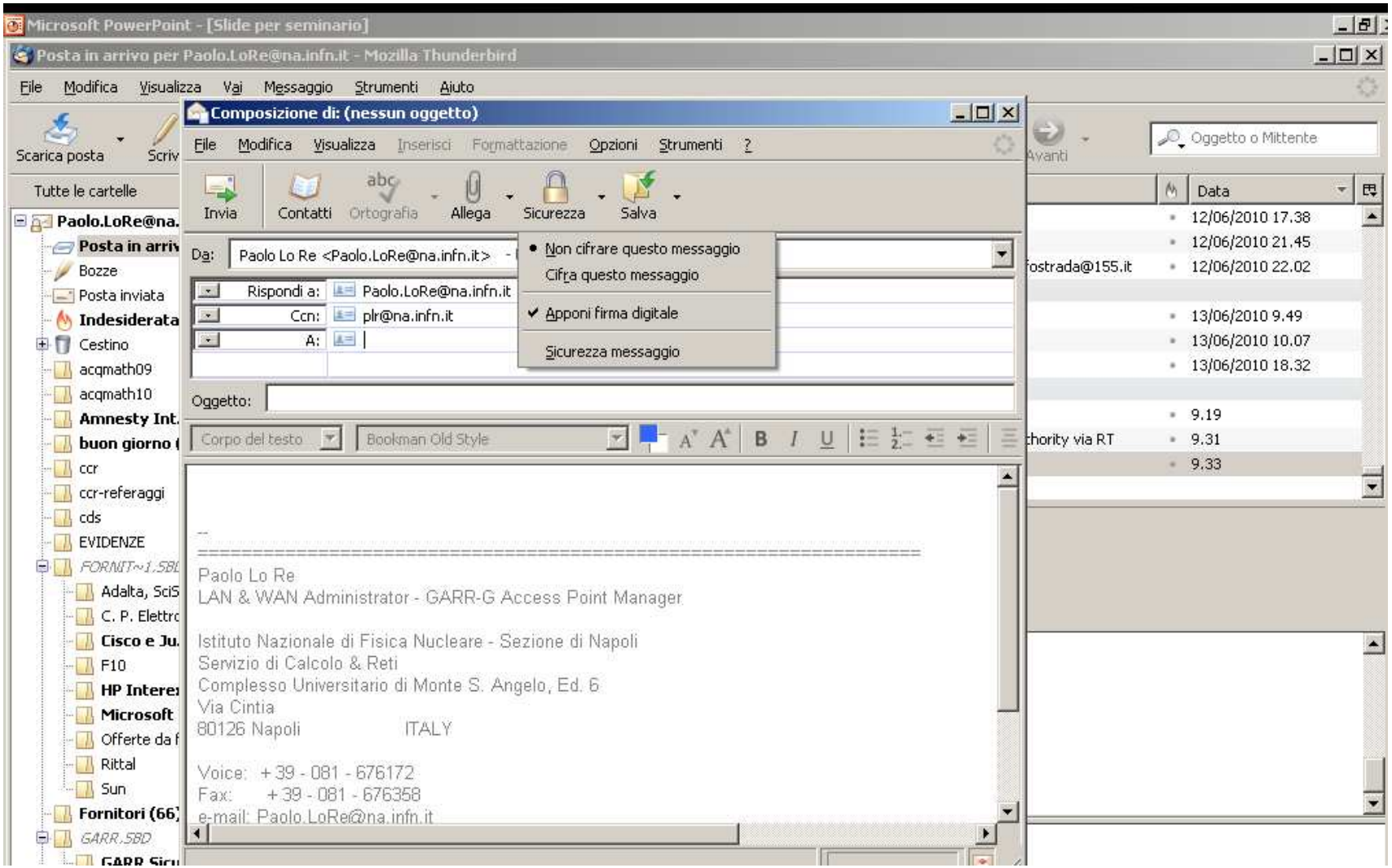


Certification Authority - 3



Paolo Lo Re, INFN Napoli, 2010

Certification Authority - 4



Sicurezza nei servizi

Il primo passo per la sicurezza nei servizi è la Sicurezza hardware (**disponibilità**)

Tutti i computer preposti ai servizi principali sono ridondati e sono implementati mediante l'utilizzo di macchine virtuali.

I più diffusi software per la realizzazione di macchine virtuali sono VMWARE (commodity) e XEN (freeware).

In forme diverse, consentono di ripristinare più o meno agevolmente un servizio compromesso da un problema hardware su una macchina fisica.

Posta elettronica e security - 1

Esistono diversi sistemi per la sicurezza della posta elettronica, che effettuano un controllo antivirus e antispam a livello centrale, agendo sulla macchina “postina”.

Un diffuso software antispam freeware è **SpamAssassin,** che utilizza filtri Bayesiani, cioè “impara” dall’esperienza.

La configurazione, tuttavia, è piuttosto complessa.

L’INFN ha adottato a livello nazionale un commodity software (cioè a pagamento), il **PureMessage** della **Sophos**.

Ha il vantaggio di aggiornarsi automaticamente dal sito Sophos sui “fingerprint” dei messaggi spam.

Non c’è invece una facile difesa pratica dal **phishing**, per cui succede a volte che messaggi di phishing raggiungono gli utenti. L’unica difesa efficace è l’”educazione” degli utenti da parte del SCR.

Posta elettronica e security - 2

Una efficace tecnica antispam consiste nel cosiddetto **Greylisting.**

All'arrivo di una email la macchina che riceve la posta simula sempre verso il mittente un sovraccarico, e quindi respinge il messaggio e ne chiede il reinvio dopo un minuto.

Il messaggio ripetuto viene accettato.

Le "normali" macchine postine ripetono il messaggio, gli spammer quasi mai.

Ciò comporta un ritardo di alcuni minuti nella consegna della posta, ma abbatte il 90% delle spam mail.

I domini postali "sicuri" possono essere elencati in una "white list" a cui non viene chiesto il reinvio e per i quali quindi non ci sono ritardi.

Indirizzamenti privati e sicurezza -1

Il Domain Name Service (DNS) presenta due livelli di approccio alla sicurezza:

- La protezione del DNS Server da problemi hardware e da attacchi software (mediante hardware duplicato e virtualizzato ed accessi alle macchine esclusi dall'esterno via ACL).

- Una efficace protezione passiva della LAN mediante l'utilizzo locale di range di indirizzi privati e non raggiungibili dall'esterno (172.16.x.y).

Indirizzamenti privati e sicurezza - 2

Gli elaboratori con indirizzo privato possono navigare in rete utilizzando la tecnica del Network Address Translation (NAT).

Anche il NAT Server è protetto da attacchi esterni con ACL sul border gateway e da guasti hardware mediante duplicazione e virtualizzazione.

Sicurezza wireless - 1

Gli accessi wireless, intrinsecamente meno sicuri, possono essere protetti in vari modi.

L'approccio più diffuso consiste nel reindirizzare gli accessi web ad una pagina di identificazione (Captive Portal).

Per l'identificazione sono comunemente usate:

- credenziali rilasciate ad personam, la cui trasmissione viene sottoposta a crittazione più o meno forte (ad es. autenticazione WPA 2 con crittografia AES);
- utilizzo di certificati elettronici X509 (opzione meno sicura).

Sicurezza wireless - 2

Eduroam e TRIP

Diverse organizzazioni si sono date regole interne di “trust relationship” per consentire l’accesso alla rete a chi si trova fuori dal suo dominio locale.

In ambito europeo è operativo il progetto Eduroam che attua il roaming automatico sulla rete accademica europea GEANT.

L’INFN ha messo in atto nelle sue sedi il progetto TRIP.

Sicurezza wireless - 3

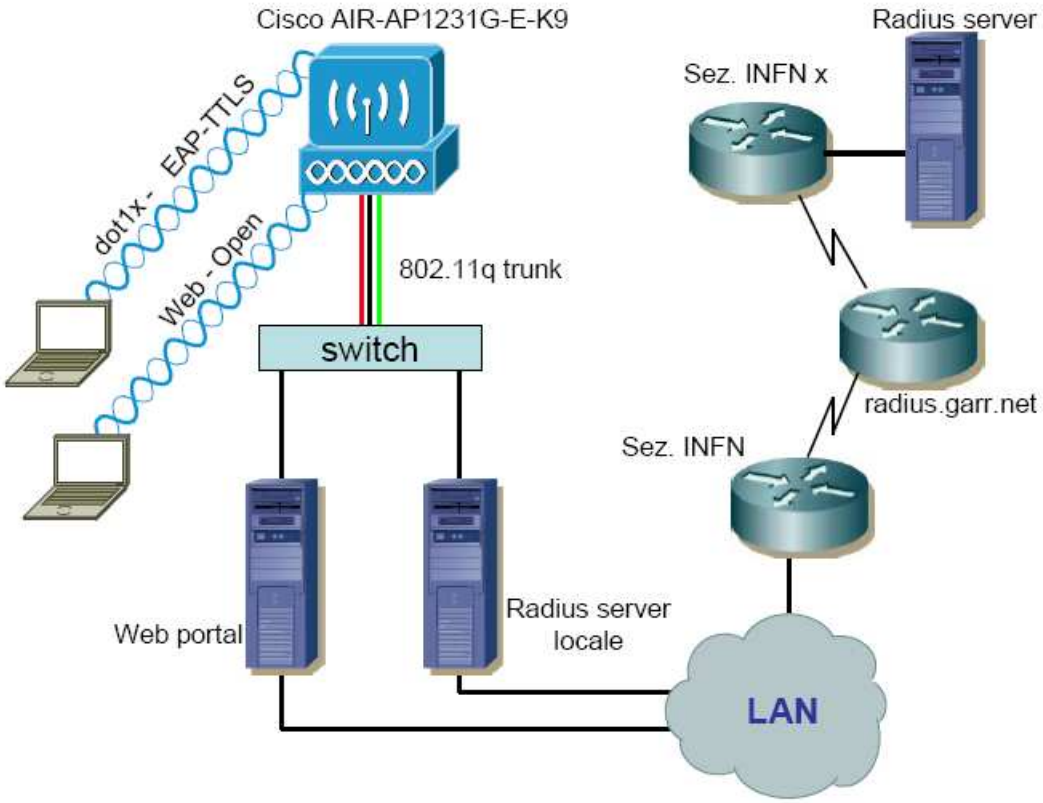
Il progetto TRIP - 1

Il progetto implementa un'architettura software e hardware che consente ad un utente di accedere alla rete INFN WiFi, dalla struttura INFN in cui si trova, mediante un'autenticazione facile e indipendente dalla rete ospitante.

L'autenticazione è riferita a due differenti tipologie di utenti: utenti INFN (dipendenti e associati) e utenti non INFN, cioè ospiti appartenenti ad altre Organizzazioni.
Per gli utenti INFN l'autenticazione si basa su EAP-TTLS che fa uso di un'architettura di server radius distribuiti.
Per gli utenti ospiti l'autenticazione è basata sull'utilizzo di un portale web.

Sicurezza wireless - 4

Il progetto TRIP - 2



Virtual Private Network

Per vari motivi può essere utile realizzare una Virtual Private Network (**VPN**) che, mediante un canale virtuale crittato, “proietta” il computer client nella network in cui risiede il server.

Diverse soluzioni commodity (commerciali) usano un hardware dedicato e un software proprietario, di solito basato su implementazioni del protocollo IPSec.

Il SCR di Napoli offre ai suoi utenti un servizio basato su software free (OpenVPN) con crittazione SSL 3.0 .

Sicurezza nel World Wide Web - 1

Ci sono in realtà 2 problemi distinti:

- **Sicurezza per chi naviga**
- **Sicurezza per il Web Server**

Sicurezza nel World Wide Web - 2

Sicurezza (e privacy) per chi naviga

- **Attenzione ai siti con certificato**

  Il browser avvisa quando l'Autorità che ha emesso il certificato è sconosciuta. Nel caso di connessioni a siti protetti (banche, ecc.) il rifiuto del certificato protegge da attacchi "man in the middle".

- **Attenzione alle connessioni crittate (https://)**

  Deve apparire il piccolo lucchetto in basso a destra!

- **Attenzione ai cookie**

  Possono "inoculare" dei Trojan Horse. Sempre – da Opzioni – chiederne la cancellazione a fine sessione.

- **Attenzione alla cronologia di navigazione**

  Può essere letta lato server. Per privacy conviene cancellarla a fine sessione o annullarla del tutto.

Sicurezza nel World Wide Web – 3

Sicurezza per il Web Server

- **Sempre tenere aggiornato il S.O. e il server**

  Protegge da problemi noti nelle versioni vecchie.
- **Attenzione ai privilegi assegnati al processo server**

  Alcuni exploits riescono ad aprire una shell che eredita i privilegi dal server. Il processo web server deve avere i minimi privilegi possibile.
- **Attenzione al data entry (form)**

  E' possibile usare le form per "Code Injection".
- **Sempre proteggere il server a livello di firewall**

  Se ogni accesso al server è chiuso tranne quelli "istituzionali", anche chi riesce a guadagnare accesso poi può solo fare danni locali al server.

IDS - 1

Esistono molti Intrusion Detection System (IDS).

Ne esistono vari che sono proattivi, cioè che eseguono azioni in risposta a determinati eventi, altri che si limitano ad inviare avvisi, ed altri infine che sono sostanzialmente dei sistemi di monitoraggio passivo, che vanno consultati da umani ai quali è lasciato il compito di intervenire se necessario.

IDS – 2

Un software molto diffuso nell'INFN e in molte Università italiane è NTOP, sviluppato da Luca Deri presso il centro SERRA dell'Università di Pisa.

E' un sistema centralizzato, Network-based, Real time, ed effettua un monitoraggio continuo e passivo.

In altri termini, è basato su un unico elaboratore che analizza in tempo reale il traffico di rete (da e per l'esterno) che passa fra la LAN e il border gateway.

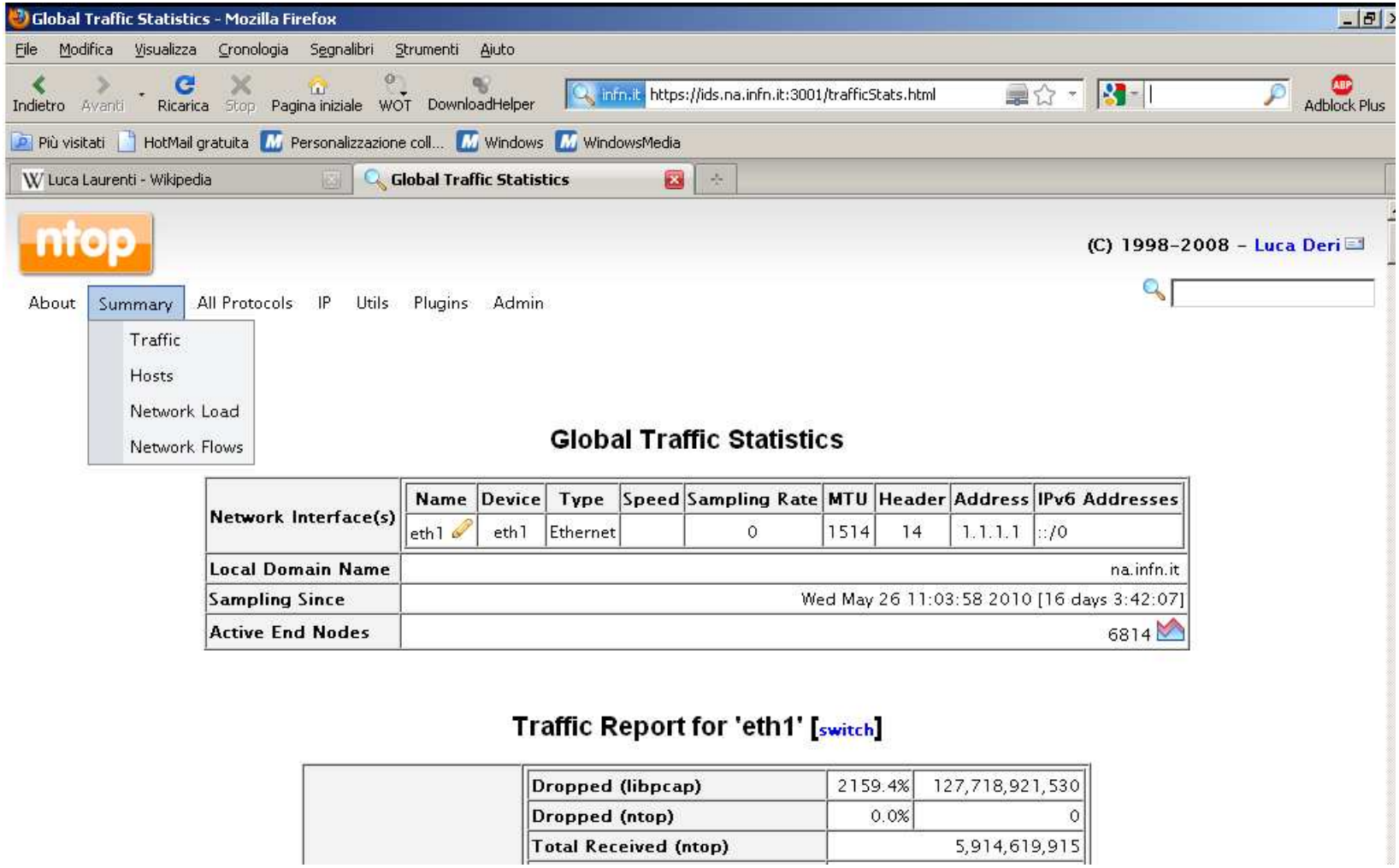
IDS - 4

Siccome non riconosce gli attacchi e non ha allarmi, NTOP NON è un IDS.

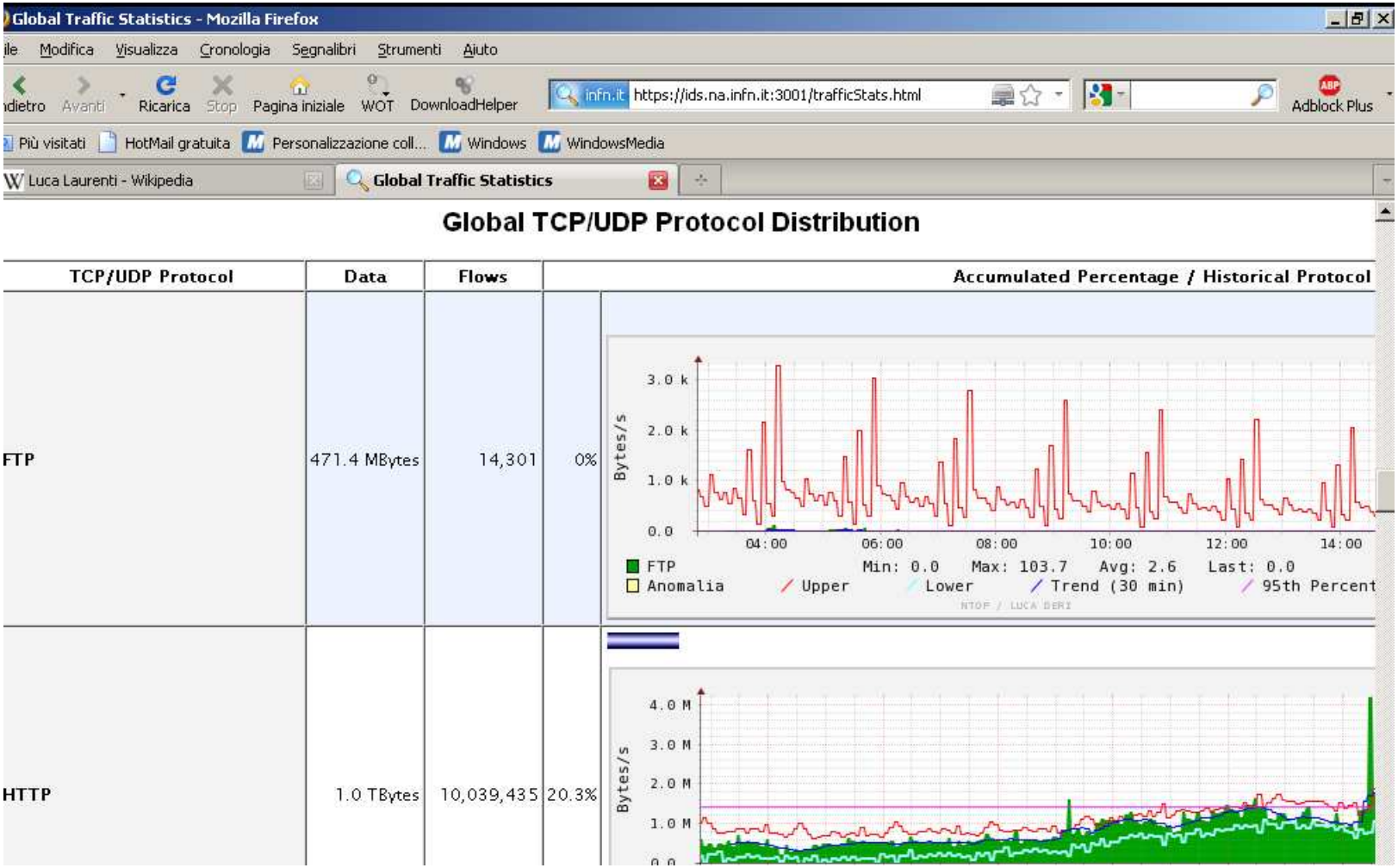
Essenzialmente è un tool per l'analisi in tempo reale del traffico di rete. Esso permette di:

- Suddividere il traffico nei vari protocolli presenti;
- Presentare analisi di traffico in base a criteri molto flessibili;
- Mostrare statistiche di traffico;
- Analizzare il traffico IP e suddividerlo in coppie provenienza <-> destinazione sia a livello di network che di singoli host.

IDS - 5

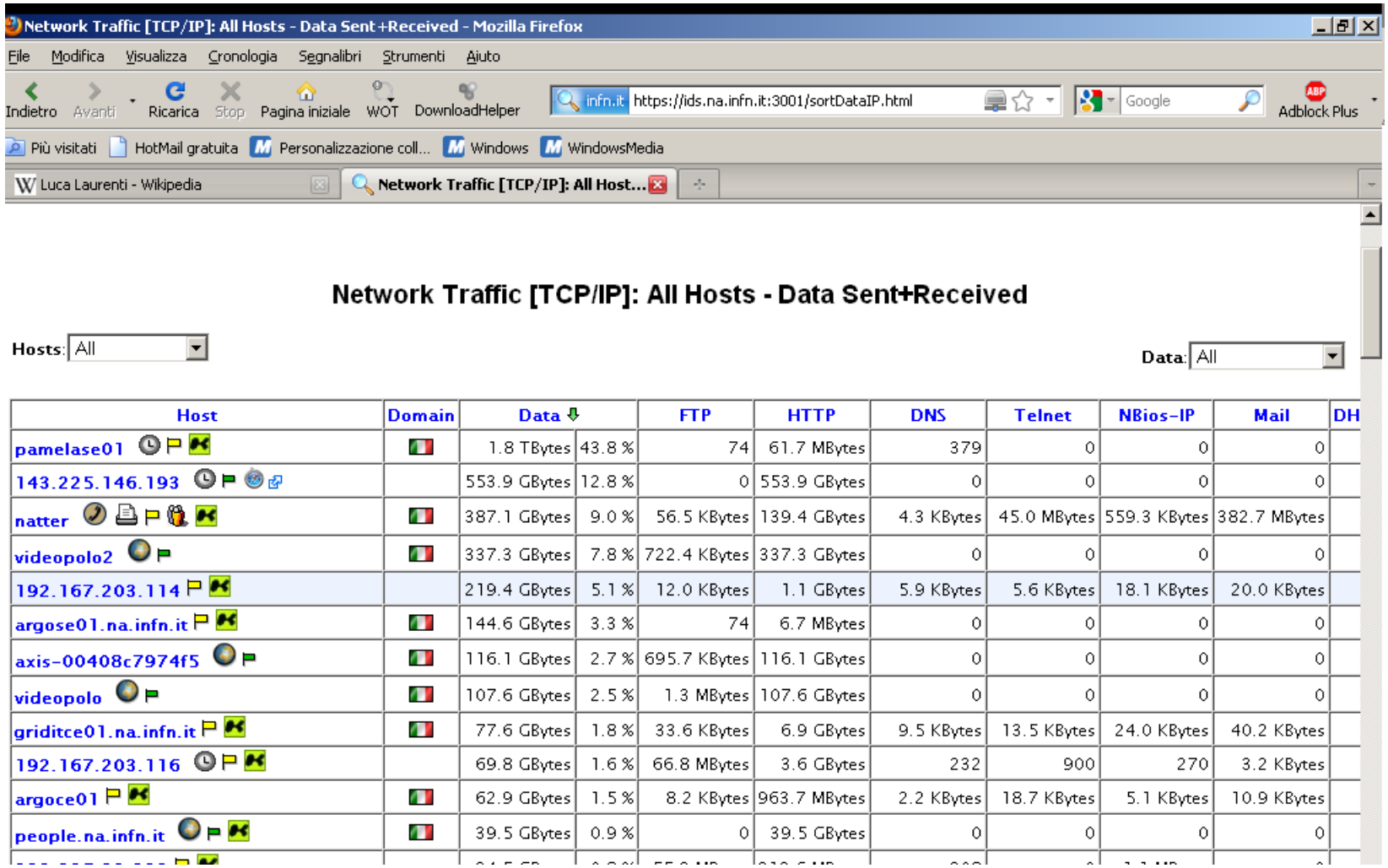

Global Traffic Statistics - Mozilla Firefox
File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto
Indietro Avanti Ricarica Stop Pagina iniziale WOT DownloadHelper
https://ids.na.infn.it:3001/trafficStats.html
Adblock Plus
Più visitati HotMail gratuita Personalizzazione coll... Windows WindowsMedia
Luca Laurenti - Wikipedia
Global Traffic Statistics
ntop
(C) 1998-2008 – Luca Deri
About Summary All Protocols IP Utils Plugins Admin
Traffic
Hosts
Network Load
Network Flows
Global Traffic Statistics
Network Interface(s)
Name Device Type Speed Sampling Rate MTU Header Address IPv6 Addresses
eth1 eth1 Ethernet 0 1514 14 1.1.1.1 ::/0
Local Domain Name
na.infn.it
Sampling Since
Wed May 26 11:03:58 2010 [16 days 3:42:07]
Active End Nodes
6814
Traffic Report for 'eth1' [switch]
Dropped (libpcap) 2159.4% 127,718,921,530
Dropped (ntop) 0.0% 0
Total Received (ntop) 5,914,619,915

IDS - 6



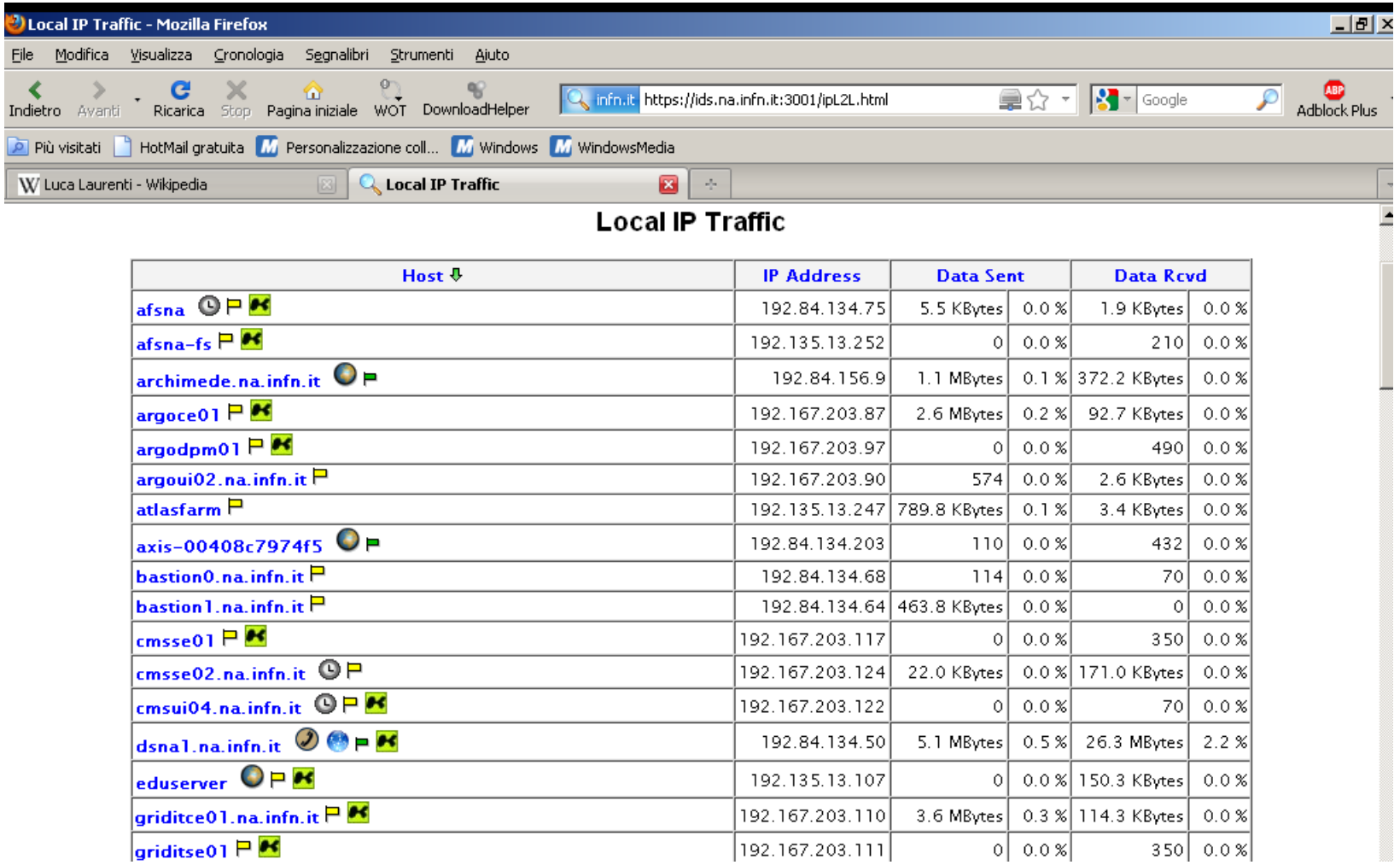
Paolo Lo Re, INFN Napoli, 2010

IDS - 7



Host	Domain	Data		FTP	HTTP	DNS	Telnet	NBios-IP	Mail	DH
pamelase01		1.8 TBytes	43.8 %	74	61.7 MBytes	379	0	0	0	
143.225.146.193		553.9 GBytes	12.8 %	0	553.9 GBytes	0	0	0	0	
natter		387.1 GBytes	9.0 %	56.5 KBytes	139.4 GBytes	4.3 KBytes	45.0 MBytes	559.3 KBytes	382.7 MBytes	
videopolo2		337.3 GBytes	7.8 %	722.4 KBytes	337.3 GBytes	0	0	0	0	
192.167.203.114		219.4 GBytes	5.1 %	12.0 KBytes	1.1 GBytes	5.9 KBytes	5.6 KBytes	18.1 KBytes	20.0 KBytes	
argose01.na.infn.it		144.6 GBytes	3.3 %	74	6.7 MBytes	0	0	0	0	
axis-00408c7974f5		116.1 GBytes	2.7 %	695.7 KBytes	116.1 GBytes	0	0	0	0	
videopolo		107.6 GBytes	2.5 %	1.3 MBytes	107.6 GBytes	0	0	0	0	
griditce01.na.infn.it		77.6 GBytes	1.8 %	33.6 KBytes	6.9 GBytes	9.5 KBytes	13.5 KBytes	24.0 KBytes	40.2 KBytes	
192.167.203.116		69.8 GBytes	1.6 %	66.8 MBytes	3.6 GBytes	232	900	270	3.2 KBytes	
argoce01		62.9 GBytes	1.5 %	8.2 KBytes	963.7 MBytes	2.2 KBytes	18.7 KBytes	5.1 KBytes	10.9 KBytes	
people.na.infn.it		39.5 GBytes	0.9 %	0	39.5 GBytes	0	0	0	0	

IDS – 8



Local IP Traffic

Host	IP Address	Data Sent		Data Rcvd	
afsna	192.84.134.75	5.5 KBytes	0.0 %	1.9 KBytes	0.0 %
afsna-fs	192.135.13.252	0	0.0 %	210	0.0 %
archimede.na.infn.it	192.84.156.9	1.1 MBytes	0.1 %	372.2 KBytes	0.0 %
argoce01	192.167.203.87	2.6 MBytes	0.2 %	92.7 KBytes	0.0 %
argodpm01	192.167.203.97	0	0.0 %	490	0.0 %
argoui02.na.infn.it	192.167.203.90	574	0.0 %	2.6 KBytes	0.0 %
atlasfarm	192.135.13.247	789.8 KBytes	0.1 %	3.4 KBytes	0.0 %
axis-00408c7974f5	192.84.134.203	110	0.0 %	432	0.0 %
bastion0.na.infn.it	192.84.134.68	114	0.0 %	70	0.0 %
bastion1.na.infn.it	192.84.134.64	463.8 KBytes	0.0 %	0	0.0 %
cmsse01	192.167.203.117	0	0.0 %	350	0.0 %
cmsse02.na.infn.it	192.167.203.124	22.0 KBytes	0.0 %	171.0 KBytes	0.0 %
cmsui04.na.infn.it	192.167.203.122	0	0.0 %	70	0.0 %
dsna1.na.infn.it	192.84.134.50	5.1 MBytes	0.5 %	26.3 MBytes	2.2 %
eduserver	192.135.13.107	0	0.0 %	150.3 KBytes	0.0 %
griditce01.na.infn.it	192.167.203.110	3.6 MBytes	0.3 %	114.3 KBytes	0.0 %
griditse01	192.167.203.111	0	0.0 %	350	0.0 %

Auditing - 1

Per una valutazione oggettiva della sicurezza delle sue reti l'INFN, scartata una costosa soluzione commerciale, si è dotata di un gruppo di Auditing interno.

Questo gruppo, formato da specialisti di rete, analizza da remoto le reti di tutte le strutture INFN utilizzando un tool di "vulnerability scanning" molto efficace, NESSUS.

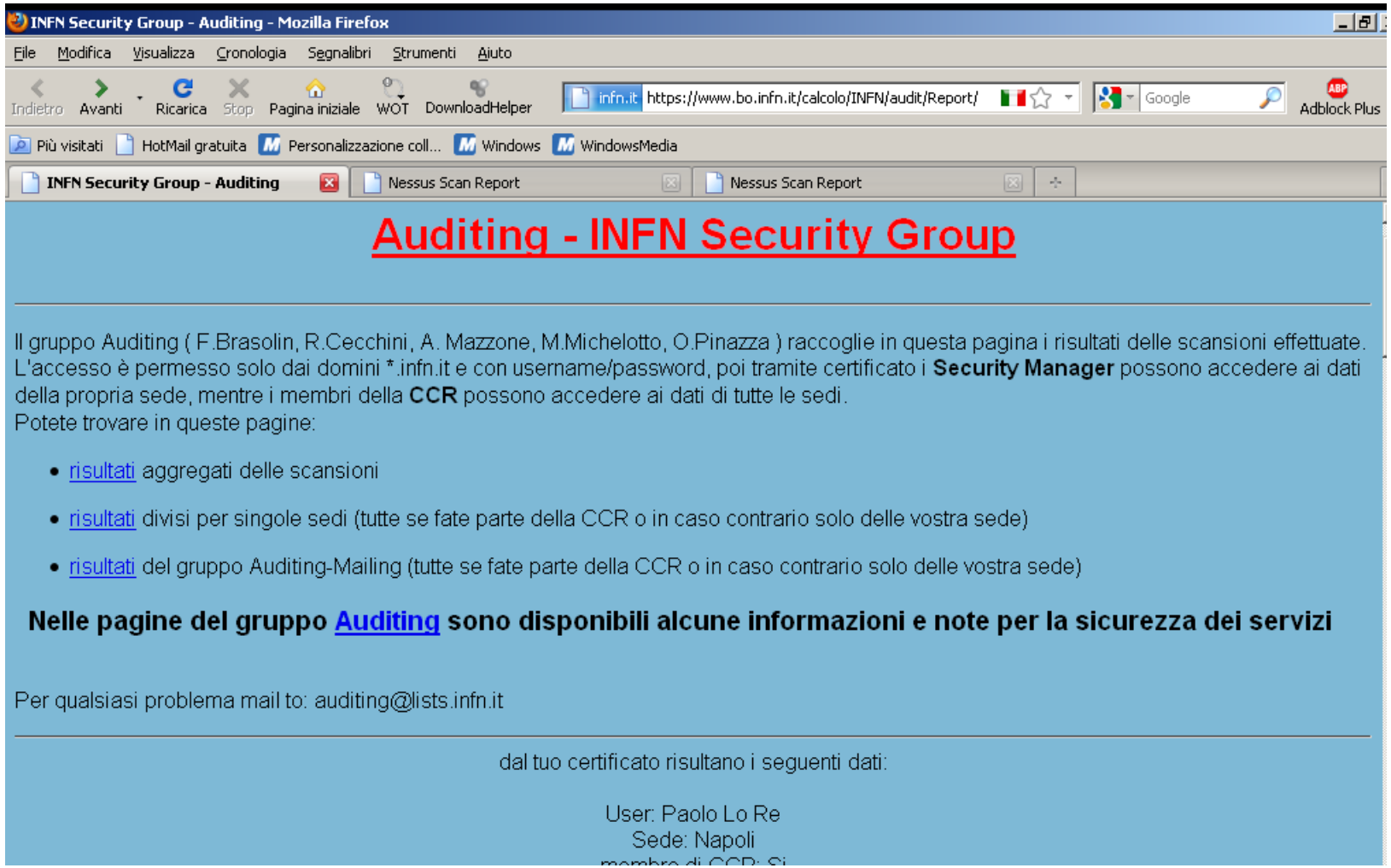
Il software analizza le reti remote sia a livello di network che di singoli host, ed evidenzia i problemi di sicurezza che riscontra.

Auditing - 2

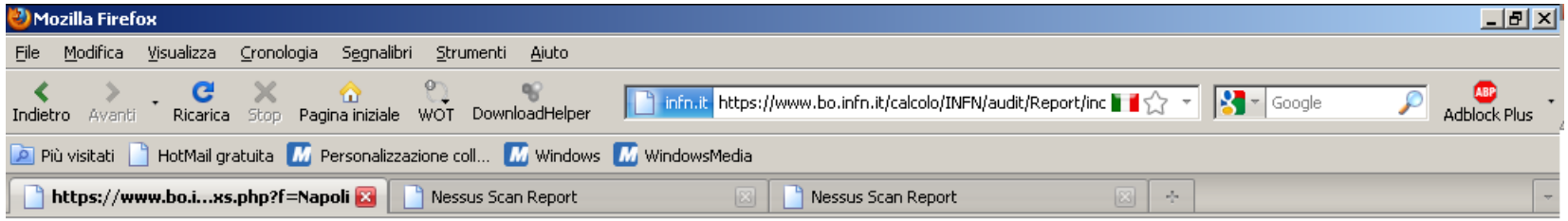
Nessus è in grado di:

- cercare i servizi di rete attivi su un elaboratore, anche su porte non standard (ad es. un web server che utilizza la porta 1234 invece della 80) o che rispondono su più porte;
- identificare le versioni dei programmi che li gestiscono;
- per ogni servizio, provare gli exploits (ossia le tecniche fraudolente di attacco informatico) che ha nel proprio database (ovviamente aggiornabile) e produrre un log citando anche le possibili tecniche di difesa;
- identificare il sistema operativo della macchina oggetto di controllo.

Auditing - 3


INFN Security Group - Auditing - Mozilla Firefox
File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto
Indietro Avanti Ricarica Stop Pagina iniziale WOT DownloadHelper
infn.it https://www.bo.infn.it/calcolo/INFN/audit/Report/
Google
Adblock Plus
Più visitati HotMail gratuita Personalizzazione coll... Windows WindowsMedia
INFN Security Group - Auditing
Nessus Scan Report
Nessus Scan Report
Auditing - INFN Security Group
Il gruppo Auditing (F.Brasolin, R.Cecchini, A. Mazzone, M.Michelotto, O.Pinazza) raccoglie in questa pagina i risultati delle scansioni effettuate.
L'accesso è permesso solo dai domini *.infn.it e con username/password, poi tramite certificato i Security Manager possono accedere ai dati della propria sede, mentre i membri della CCR possono accedere ai dati di tutte le sedi.
Potete trovare in queste pagine:
risultati aggregati delle scansioni
risultati divisi per singole sedi (tutte se fate parte della CCR o in caso contrario solo delle vostra sede)
risultati del gruppo Auditing-Mailing (tutte se fate parte della CCR o in caso contrario solo delle vostra sede)
Nelle pagine del gruppo Auditing sono disponibili alcune informazioni e note per la sicurezza dei servizi
Per qualsiasi problema mail to: auditing@lists.infn.it
dal tuo certificato risultano i seguenti dati:
User: Paolo Lo Re
Sede: Napoli

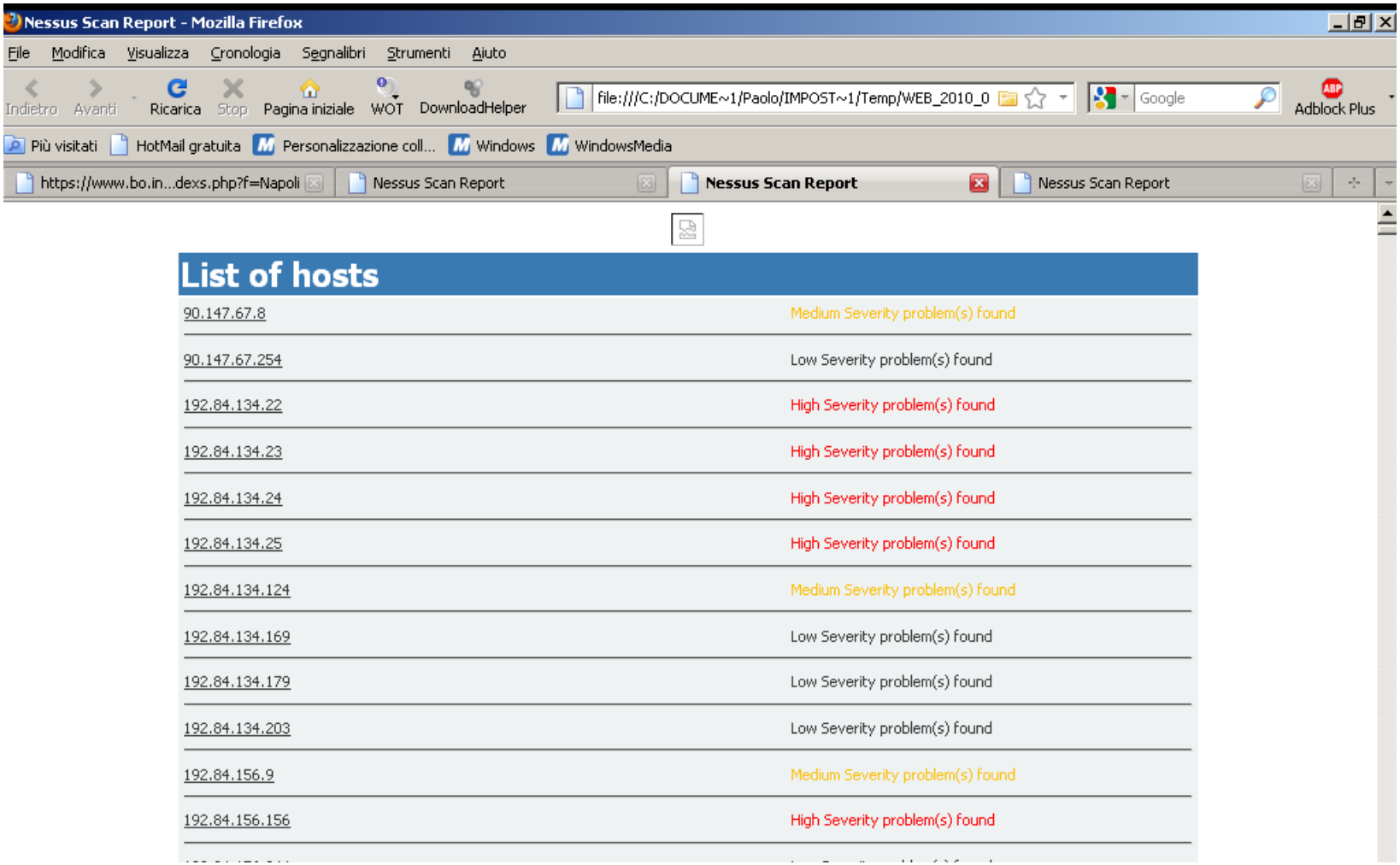
Auditing - 4



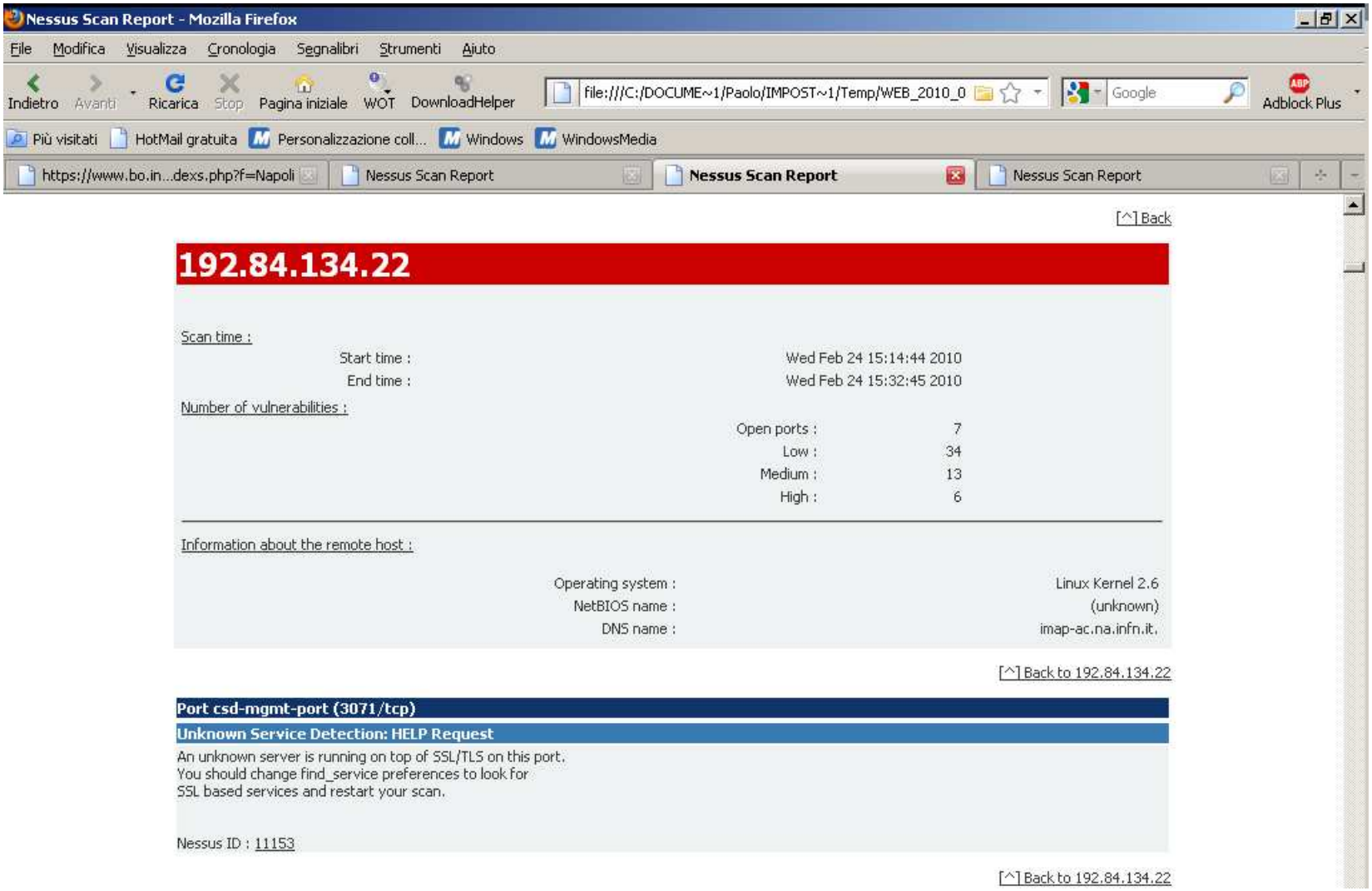
Nella tabella potrai trovare i risultati per la sede INFN: Napoli

DNS_2008_07-INFN-NA-nessus.html 7072 Byte
DNS_2009_09-INFN-NA-nessus.html 16576 Byte
DNS_2010_02-INFN-NA-nessus.html 26734 Byte
SSH_2008_11-INFN-NA-nessus.html 59249 Byte
SSH_2009_05-INFN-NA-nessus.html 102152 Byte
SSH_2009_07-INFN-NA-nessus.html 34039 Byte
SSH_2010-02-INFN-NA-nessus.html 348328 Byte
WEB_2008_03-INFN-NA-nessus.html 527558 Byte
WEB_2009_05-INFN-NA-nessus.html 568413 Byte
WEB_2009_07-INFN-NA-nessus.html 554941 Byte
WEB_2010_02-INFN-NA-nessus.html 974068 Byte
WIN_2010_05-NA-nessus.html 17841 Byte

Auditing - 5


Nessus Scan Report - Mozilla Firefox
File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto
Indietro Avanti Ricarica Stop Pagina iniziale WOT DownloadHelper
file:///C:/DOCUME~1/Paolo/IMPOST~1/Temp/WEB_2010_0
Google
Adblock Plus
Più visitati HotMail gratuita Personalizzazione coll... Windows WindowsMedia
https://www.bo.in...dexs.php?f=Napoli
Nessus Scan Report
Nessus Scan Report
Nessus Scan Report
List of hosts
90.147.67.8 Medium Severity problem(s) found
90.147.67.254 Low Severity problem(s) found
192.84.134.22 High Severity problem(s) found
192.84.134.23 High Severity problem(s) found
192.84.134.24 High Severity problem(s) found
192.84.134.25 High Severity problem(s) found
192.84.134.124 Medium Severity problem(s) found
192.84.134.169 Low Severity problem(s) found
192.84.134.179 Low Severity problem(s) found
192.84.134.203 Low Severity problem(s) found
192.84.156.9 Medium Severity problem(s) found
192.84.156.156 High Severity problem(s) found

Auditing - 6


Nessus Scan Report - Mozilla Firefox
File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto
Indietro Avanti Ricarica Stop Pagina iniziale WOT DownloadHelper
file:///C:/DOCUME~1/Paolo/IMPOST~1/Temp/WEB_2010_0
Google
Adblock Plus
Più visitati HotMail gratuita Personalizzazione coll... Windows WindowsMedia
https://www.bo.in...dexs.php?f=Napoli
Nessus Scan Report
Nessus Scan Report
Nessus Scan Report
[^] Back
192.84.134.22
Scan time :
Start time : Wed Feb 24 15:14:44 2010
End time : Wed Feb 24 15:32:45 2010
Number of vulnerabilities :
Open ports : 7
Low : 34
Medium : 13
High : 6
Information about the remote host :
Operating system : Linux Kernel 2.6
NetBIOS name : (unknown)
DNS name : imap-ac.na.infn.it.
[^] Back to 192.84.134.22
Port csd-mgmt-port (3071/tcp)
Unknown Service Detection: HELP Request
An unknown server is running on top of SSL/TLS on this port.
You should change find_service preferences to look for
SSL based services and restart your scan.
Nessus ID : 11153
[^] Back to 192.84.134.22