I nuovi servizi TCS e SCARR

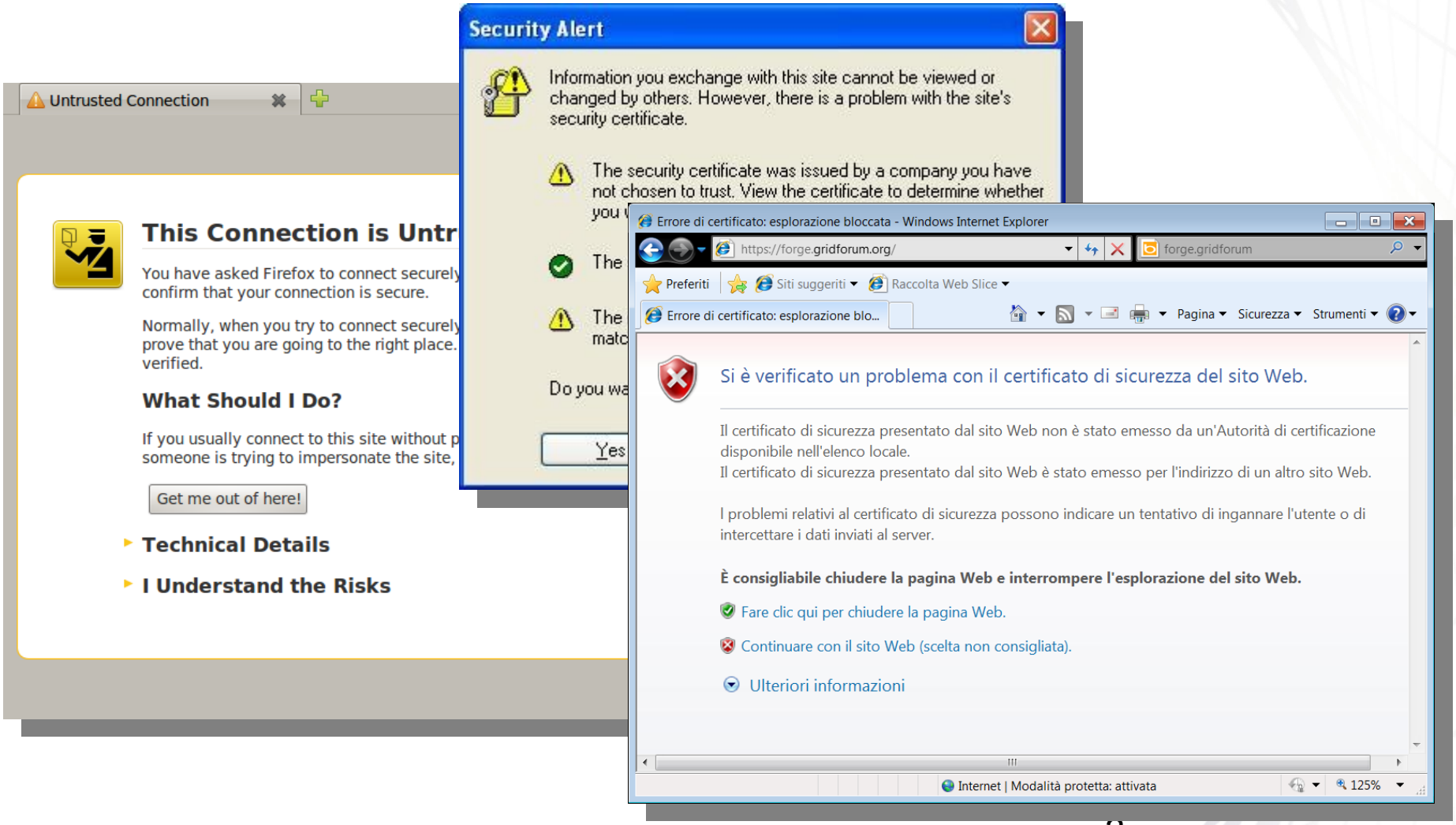
Roberto Cecchini - GARR

Consortium GARR

TCS
Terena Certificate Service

Consortium GARR

Il problema


Untrusted Connection
This Connection is Untr
You have asked Firefox to connect securely
confirm that your connection is secure.
Normally, when you try to connect securely
prove that you are going to the right place.
verified.
What Should I Do?
If you usually connect to this site without p
someone is trying to impersonate the site,
Get me out of here!
Technical Details
I Understand the Risks
Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you
The
The
matc
Do you wa
Yes
Errore di certificato: esplorazione bloccata - Windows Internet Explorer
https://forge.gridforum.org/
forge.gridforum
Preferiti
Siti suggeriti
Raccolta Web Slice
Errore di certificato: esplorazione blo...
Pagina
Sicurezza
Strumenti
Si è verificato un problema con il certificato di sicurezza del sito Web.
Il certificato di sicurezza presentato dal sito Web non è stato emesso da un'Autorità di certificazione disponibile nell'elenco locale.
Il certificato di sicurezza presentato dal sito Web è stato emesso per l'indirizzo di un altro sito Web.
I problemi relativi al certificato di sicurezza possono indicare un tentativo di ingannare l'utente o di intercettare i dati inviati al server.
È consigliabile chiudere la pagina Web e interrompere l'esplorazione del sito Web.
Fare clic qui per chiudere la pagina Web.
Continuare con il sito Web (scelta non consigliata).
Ulteriori informazioni
Internet | Modalità protetta: attivata
125%

La soluzione

- TCS: TERENA Certificate Service
  http://ca.garr.it/TCS/
  https://www.terena.org/activities/tcs/
- Certificati (x.509) rilasciati da Comodo CA (presente in tutti i più diffusi browser)
  - gratuiti per i membri GARR (un “Secure Site” per 3 anni costa circa 1k$)

Tipi di certificato

- Server
  - 1, 2 o 3 anni
  - nomi multipli
- Server e-science
- Personali
- Personali e-science

} riservati ai membri IDEM

Come ottenerli

- Istruzioni: http://ca.garr.it/TCS/
  - e anche i corsi GARR CA: http://ca.garr.it/corso.php
- Due responsabili per organizzazione
  - devono approvare (mail firmato) le richieste per server
- Tutte le procedure sono online
  - per i certificati personali è necessaria l'autenticazione dall'IdP dell'Organizzazione

SCARR
Scansioni ripetute a richiesta

Consortium GARR

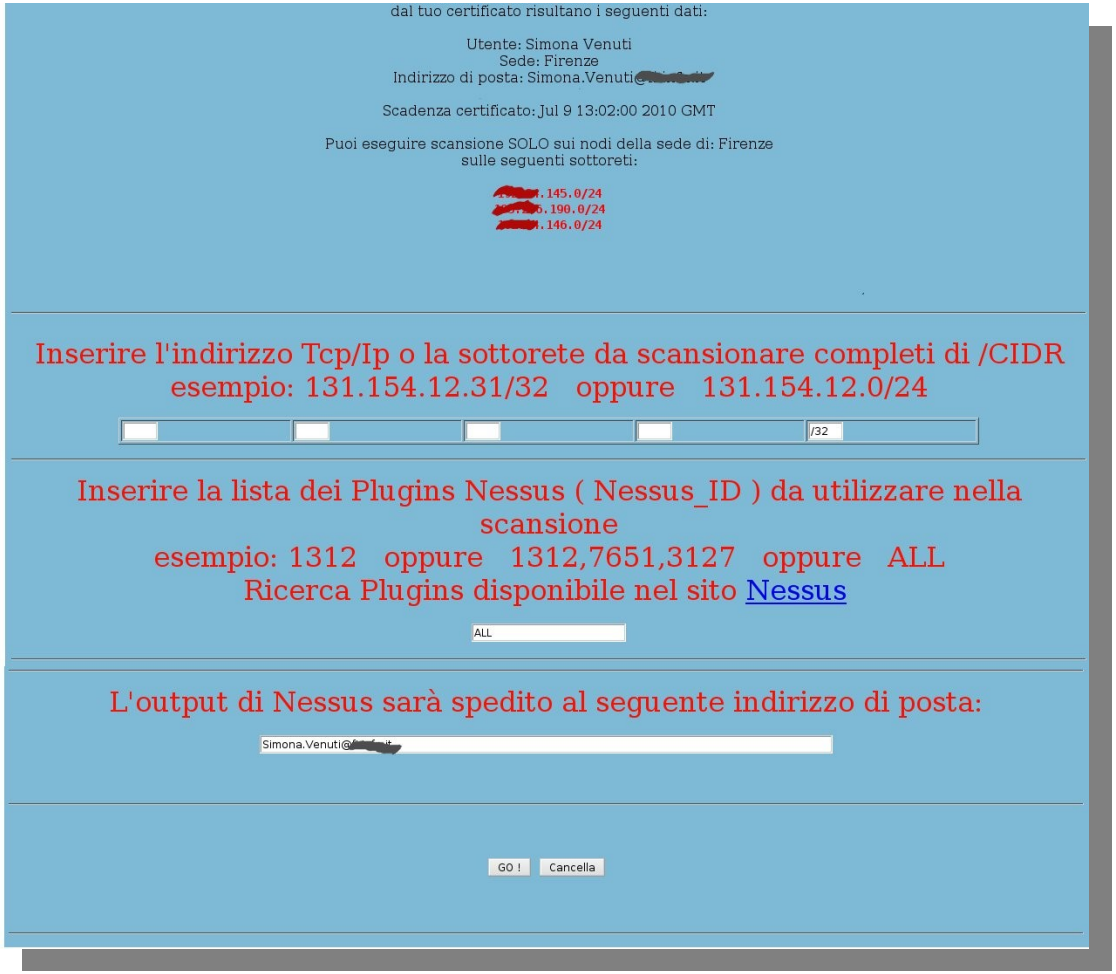
Cosa?

- Scansioni dei propri nodi, dall'esterno, alla ricerca di vulnerabilità
  - **nessus** (per ora)
- Prenotazione online
  - ringraziamo Franco Brasolin (INFN, Bologna)
- Risultati via mail

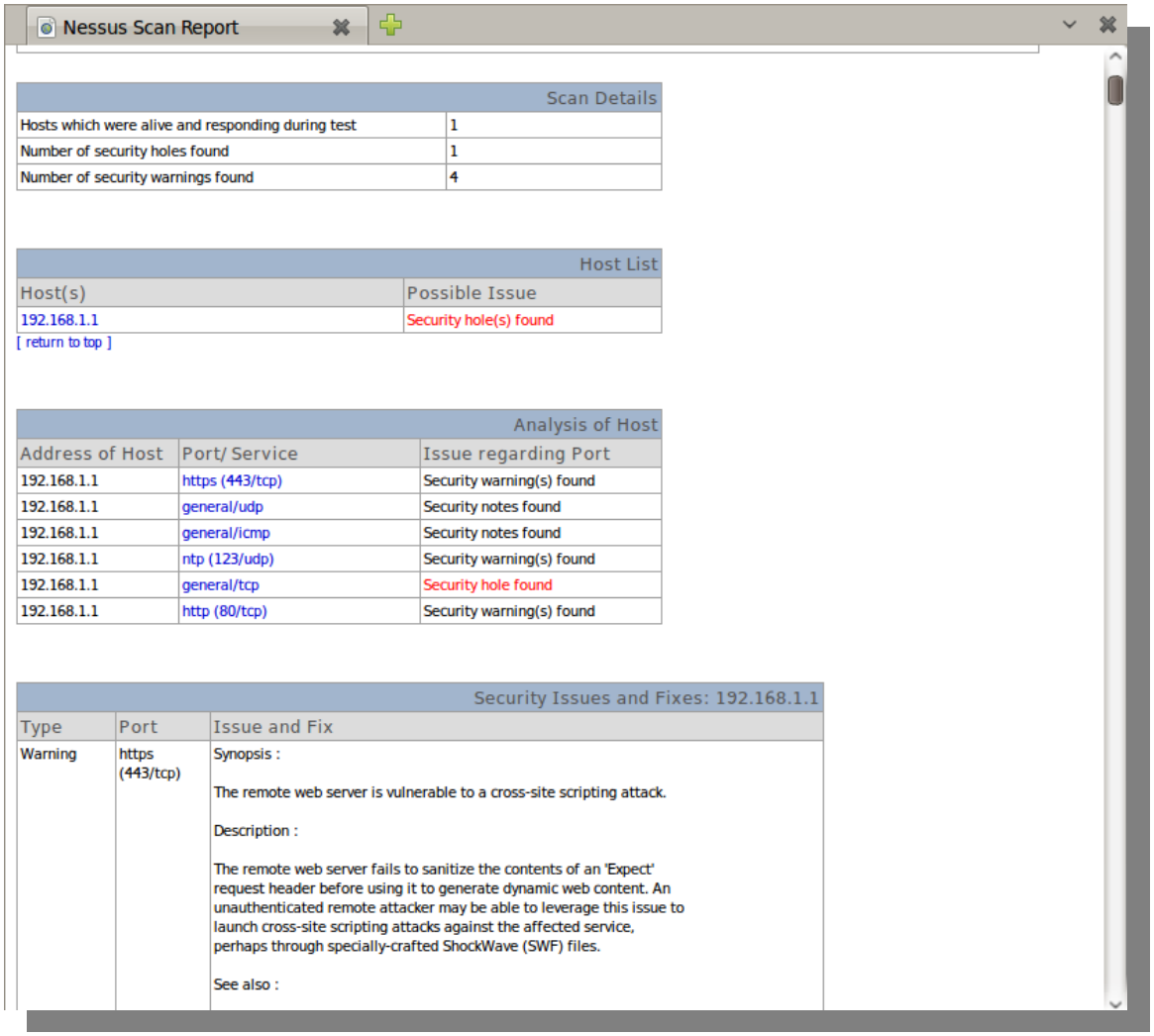
Chi?

- Riservato agli APM (per le loro reti...)
  - membri IDEM
  - certificato GARR CA

Richiesta


dal tuo certificato risultano i seguenti dati:
Utente: Simona Venuti
Sede: Firenze
Indirizzo di posta: Simona.Venuti
Scadenza certificato: Jul 9 13:02:00 2010 GMT
Puoi eseguire scansione SOLO sui nodi della sede di: Firenze
sulle seguenti sottoreti:
.145.0/24
.190.0/24
.146.0/24
Inserire l'indirizzo Tcp/Ip o la sottorete da scansionare completi di /CIDR
esempio: 131.154.12.31/32 oppure 131.154.12.0/24
/32
Inserire la lista dei Plugins Nessus (Nessus_ID) da utilizzare nella scansione
esempio: 1312 oppure 1312,7651,3127 oppure ALL
Ricerca Plugins disponibile nel sito Nessus
ALL
L'output di Nessus sarà spedito al seguente indirizzo di posta:
Simona.Venuti
GO !
Cancella

Risposta



Nessus Scan Report

Scan Details	
Hosts which were alive and responding during test	1
Number of security holes found	1
Number of security warnings found	4

Host List	
Host(s)	Possible Issue
192.168.1.1	Security hole(s) found

[return to top]

Analysis of Host		
Address of Host	Port/ Service	Issue regarding Port
192.168.1.1	https (443/tcp)	Security warning(s) found
192.168.1.1	general/udp	Security notes found
192.168.1.1	general/icmp	Security notes found
192.168.1.1	ntp (123/udp)	Security warning(s) found
192.168.1.1	general/tcp	Security hole found
192.168.1.1	http (80/tcp)	Security warning(s) found

Security Issues and Fixes: 192.168.1.1		
Type	Port	Issue and Fix
Warning	https (443/tcp)	Synopsis : The remote web server is vulnerable to a cross-site scripting attack. Description : The remote web server fails to sanitize the contents of an 'Expect' request header before using it to generate dynamic web content. An unauthenticated remote attacker may be able to leverage this issue to launch cross-site scripting attacks against the affected service, perhaps through specially-crafted ShockWave (SWF) files. See also :