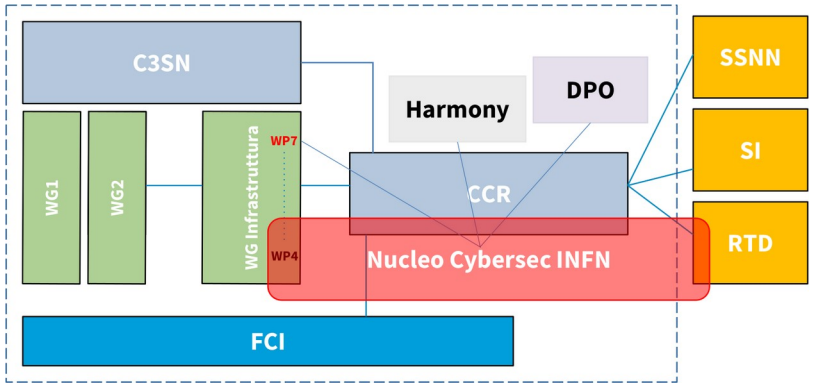
Istituto Nazionale di Fisica Nucleare
NUcleo CyberSecurity

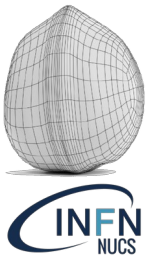
Interfaccia web per la gestione delle vulnerabilità

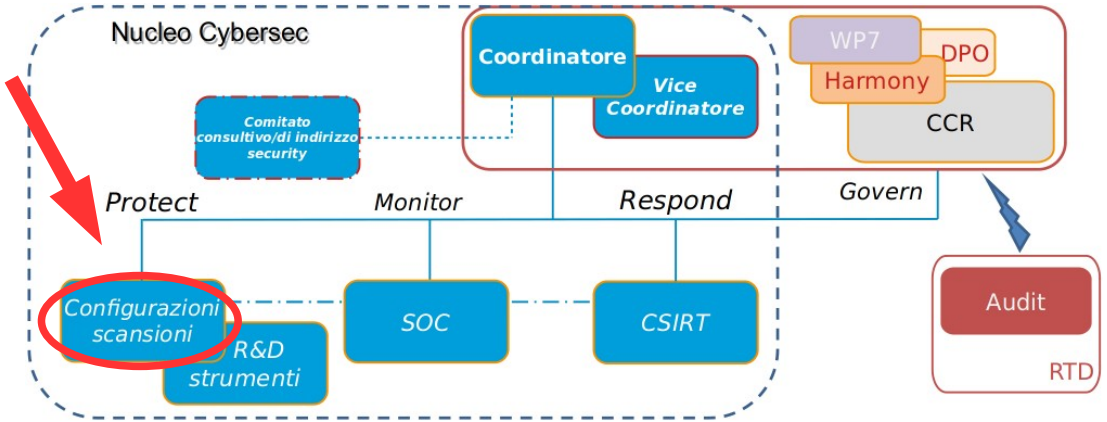
Leandro Lanzi

Workshop sul Calcolo nell'INFN
Loano, 22 - 26 maggio 2023

Collocazione del presente lavoro







- Il **NUcleo Cyber Security** (NUCS) si occupa di tutti gli aspetti legati alla sicurezza informatica dell'INFN.
- In particolare il NUCS ha il compito di dotare l'Ente di strumenti organizzativi, procedurali ed operativi, nonché di un'infrastruttura centrale per la gestione di tutti gli aspetti della cybersicurity: **protezione**, **controllo**, **risposta** e **governo**.
- All'interno dell'attività di protezione del NUCS sono previste **scansioni di sicurezza** di tutti i sistemi informatici per
  - **monitorare** tutti i servizi esposti ad eventuali attacchi informatici,
  - **rilevare e notificare** agli interessati eventuali vulnerabilità potenzialmente utilizzabili per compromettere tali servizi,
  - **vigilare e verificare** le operazioni di correzione delle vulnerabilità segnalate.

Collocazione temporale

Miniworkshop sulla Sicurezza Informatica
(Padova, 13-15/02/23)

Armonizzare l'attività delle scansioni di vulnerabilità in ambito CCR e INFN-Cloud e automazione dei processi

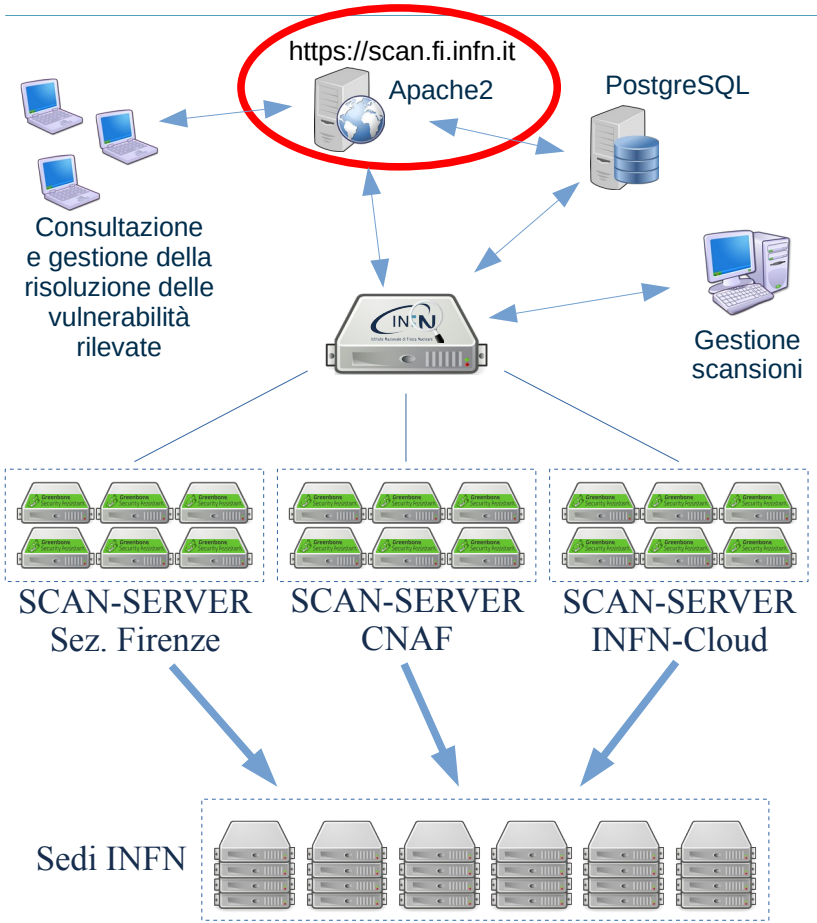
- Si intende realizzare **un'unica piattaforma** web ed **un'unica procedura per la gestione di scansioni** sufficientemente flessibile da permettere ad INFN-Cloud di mantenere il suo attuale livello di efficienza nella **gestione della singola vulnerabilità sul singolo IP** ma anche di essere utilizzata a livello nazionale per migliorare il monitoraggio delle procedure di risoluzione delle vulnerabilità che attualmente mostra grande criticità.

Riunione della Commissione Calcolo e Reti
(Roma, 20-22/03/2023)

Programma di massima

Data	Milestone
[illegible]	[illegible]
[illegible]	[illegible]
agosto	[illegible] SCANSIONI a regime
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]

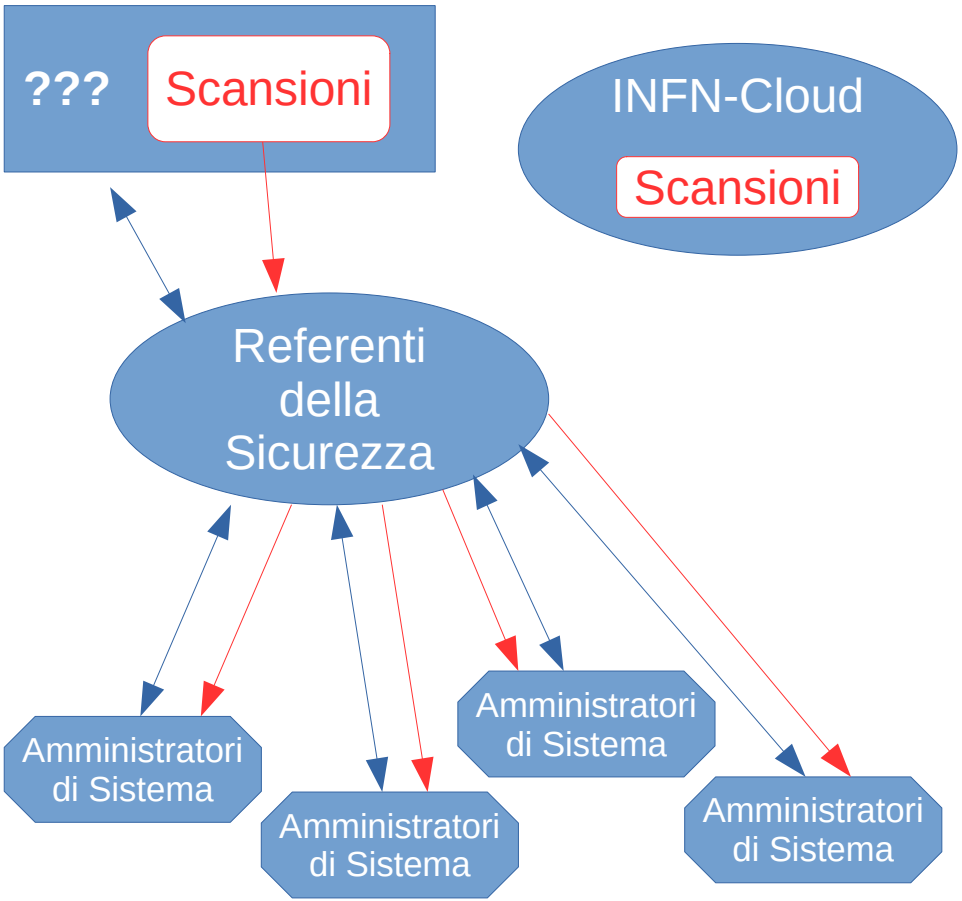
Scansioni di sicurezza del NUCS



- Il NUCS sta utilizzando 18 macchine SCAN-SERVER (6 al CNAF, 6 su INFN-Cloud e 6 alla Sezione di Firenze) per effettuare scansioni si sicurezza su tutta la rete INFN (attualmente circa 60.000 IP, circa 3.500 nodi risultati attivi su scansioni effettuate dall'esterno delle sedi) tramite:
  - **zmap** per la rilevazione di host esposti e relativi servizi attivi (solo TCP) ;
  - **nmap**, per la rilevazione e caratterizzazione di host esposti e relativi servizi attivi;
  - **Greenbone Community Edition (GCE)** per la rilevazione di vulnerabilità di sicurezza sugli host esposti.

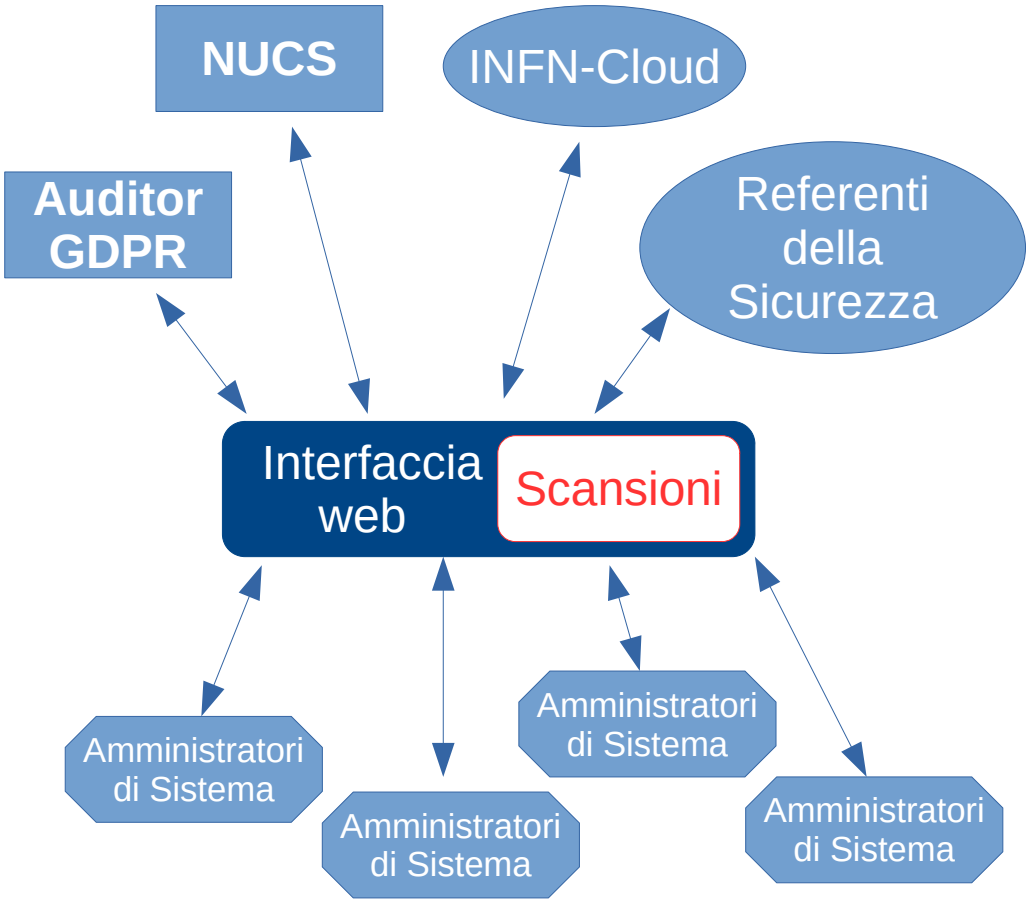
Situazione passata/attuale

- I Referenti della Sicurezza delle varie Strutture INFN, che spesso sono un sottogruppo del personale dei Servizi Calcolo e Reti, non amministrano direttamente tutti gli host della propria rete che espongono servizi all'esterno.
- Allo stato attuale il NUCS non conosce gli Amministratori di Sistema dei singoli host su cui vengono rilevate le vulnerabilità per cui è costretto a segnalarle ai Referenti della Sicurezza delle varie Strutture che subiscono il compito di fare da tramite fra NUCS ed Amministratori di Sistema.
- La situazione di INFN-Cloud è diversa in quanto le vulnerabilità vengono già notificate ad i diretti interessati.



Obiettivi della procedura di gestione delle vulnerabilità

- Gli obiettivi della procedura gestita tramite l'interfaccia web in questione sono:
  - automatizzare tutti i processi per ridurre al minimo qualsiasi interazione esterna alla piattaforma web (e-mail, telefono, video-conf, ...) da parte di tutti i soggetti interessati alla correzione delle vulnerabilità;
  - limitare al massimo l'interazione del NUCS con i Referenti della Sicurezza delle varie Strutture;
  - tener traccia dell'avanzamento nell'attività di correzione delle vulnerabilità;
  - segnalare direttamente ai diretti interessati, cioè agli Amministratori di Sistema, le vulnerabilità rilevate;
  - tenere aggiornati i Referenti della Sicurezza sullo stato di avanzamento delle correzioni delle vulnerabilità e richiederne l'intervento solo in caso di inadempienza da parte degli Amministratori di Sistema.
  - Permettere agli Auditor GDPR di accedere ai dati relativi alle vulnerabilità.



Deleghe e assegnazioni a due livelli

- Per arrivare a segnalare direttamente ai diretti interessati, cioè agli Amministratori di Sistema dei singoli host, le vulnerabilità rilevate, l'interfaccia web sfrutta il meccanismo delle **deleghe**.
- Inizialmente tutti gli host di una rete sono assegnati ai Referenti della Sicurezza della Struttura di cui la rete fa parte (primo livello di assegnazioni).
- I Referenti della Sicurezza possono assegnare i singoli host ed intere reti ad i relativi Amministratori di Sistema (secondo livello di assegnazioni).

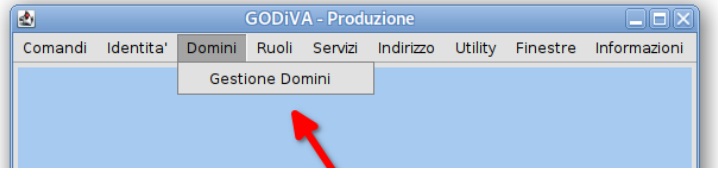
Assegnazioni di primo livello [1/2]

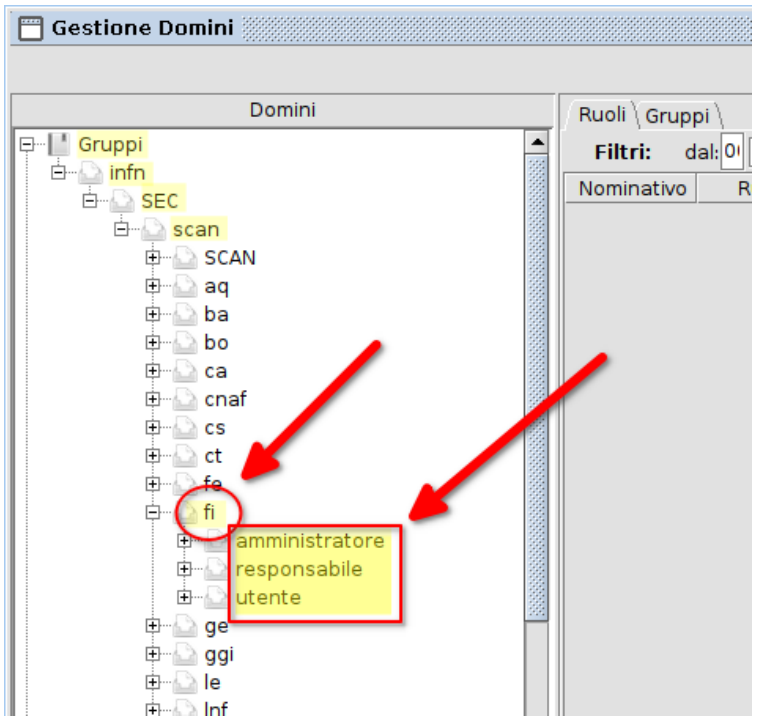
- La designazione dei Referenti della Sicurezza viene fatta tramite INFN-AAI, in GODiVA-GUI: **Domini** > **Gestione Domini**.
- Ogni Struttura è identificata nei Domini di INFN-AAI in:

  Gruppo > **infn** > **SEC** > **scan**.
- Per esempio la Sezione di Firenze è identificata da:

  Gruppo > **infn** > **SEC** > **scan** > **fi**.
- Per ogni struttura sono definiti i seguenti ruoli:
  - **responsabile**,
  - **amministratore**,

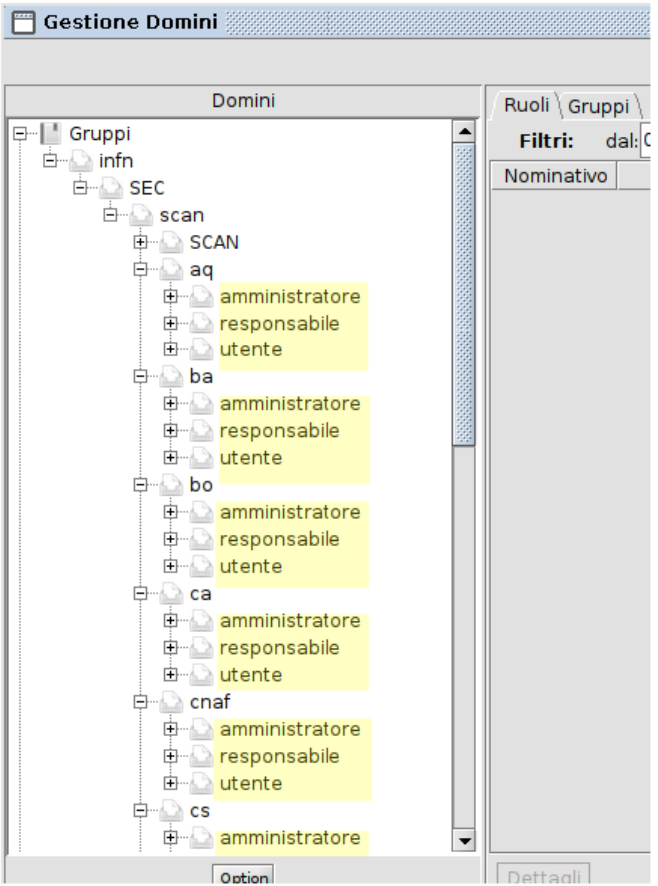
  Accesso completo ai dati e alle operazioni di correzione delle scansioni
  - **utente**. → ***Consultazione*** dei dati delle scansioni e dello stato di avanzamento delle operazioni di correzione
- Salvo casi particolari i ruoli di responsabile, amministratore ed utente devono esser **definiti in base ad un ruolo degli utenti** in INFN-AAI e non al loro nome.





Assegnazioni di primo livello [2/2]

- I Referenti della Sicurezza sono gli Amministratori.
- Configurazione di default per tutte le Strutture è la seguente:
  - **Responsabile** → Responsabile del Servizio Calcolo e Reti **Accesso completo ai dati e alle operazioni di correzione delle scansioni**
  - **Amministratore** *(Referente della Sicurezza)* → Personale del Servizio Calcolo e Reti **Accesso completo ai dati e alle operazioni di correzione delle scansioni**
  - **Utenti** → Consultazione dei dati delle scansioni e dello stato di avanzamento delle operazioni di correzione
- Il Responsabile può modificare l'elenco degli Amministratori, cioè può definire chi sono i Referenti della Sicurezza, e l'elenco degli Utenti.
- Gli Amministratori, cioè i Referenti della Sicurezza, possono modificare l'elenco degli Utenti.
- Responsabile, Amministratori ed Utenti accedono a tutti i dati delle scansioni per la propria Struttura e possono partecipare alle operazioni di gestione delle vulnerabilità.

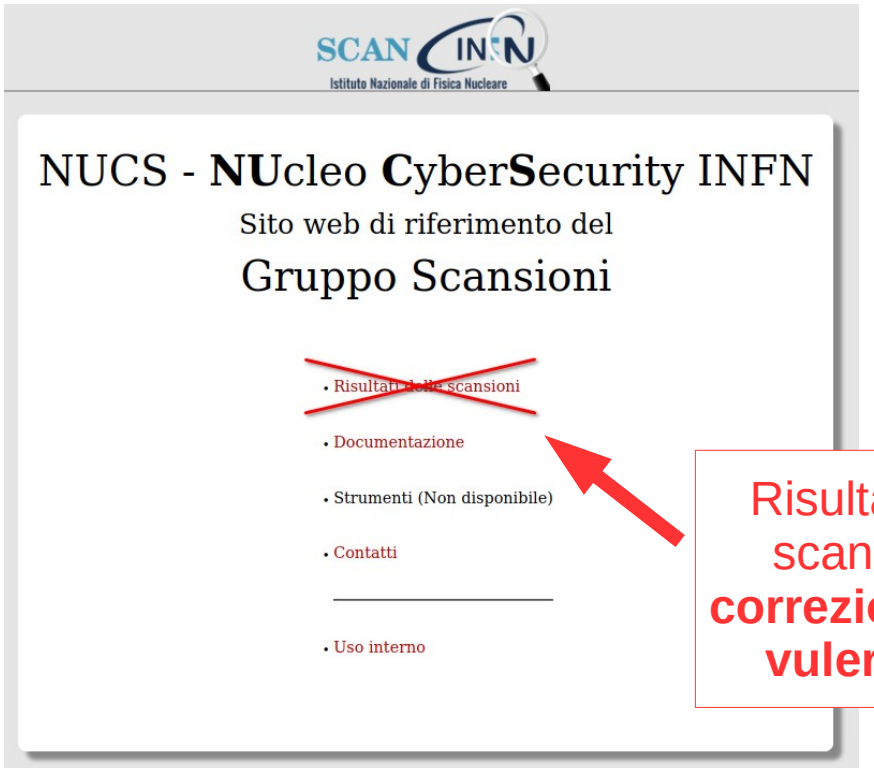


Assegnazioni di secondo livello: deleghe

- Il Responsabile e gli Amministratori (assegnazioni di primo livello) possono delegare agli Amministratori di Sistema la gestione degli host che hanno in carico (assegnazioni di secondo livello).
- Sono previste 3 procedure per assegnare le deleghe nell'interfaccia web.
  1) Scegliendo gli IP e gli utenti dall'interfaccia web.
  2) Caricando un file di testo nell'interfaccia web.
  3) Inviando tramite `scp` un file di testo al server web, dopo aver caricato una chiave pubblica SSH nell'interfaccia web, per poter automatizzare il processo di delega (pensato per INFN-Cloud ma utilizzabile da tutte le Sedi).

Accesso all'interfaccia web

https://scan.fi.infn.it



Risultati delle scansioni e **correzione delle vulerabilità**

Login ed Home page

Assegnazione di primo livello

Risultati delle scansioni

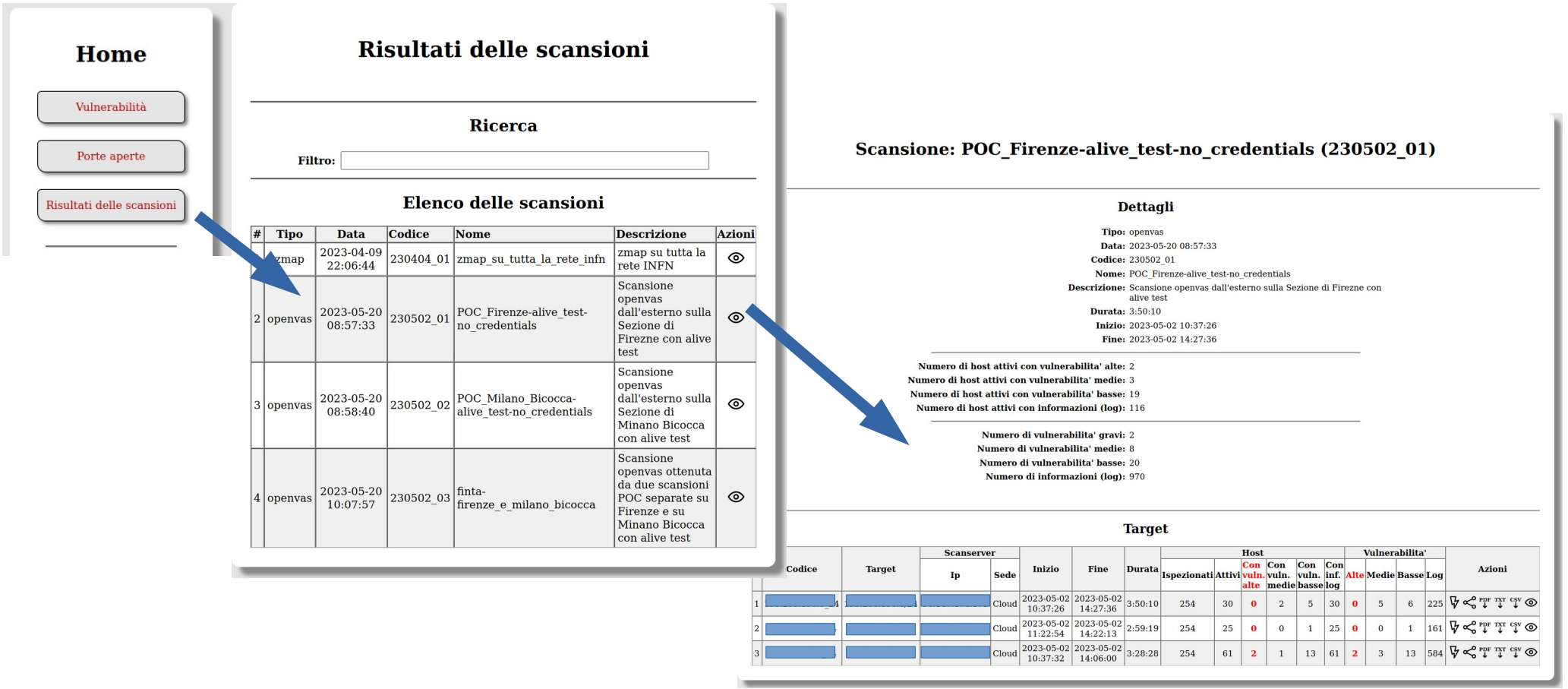
Consultazione e **gestione** di tutte le vulnerabilità rilevate su tutti gli host e le reti in carico

Consultazione di tutte le porte aperte su tutti gli host e le reti in carico

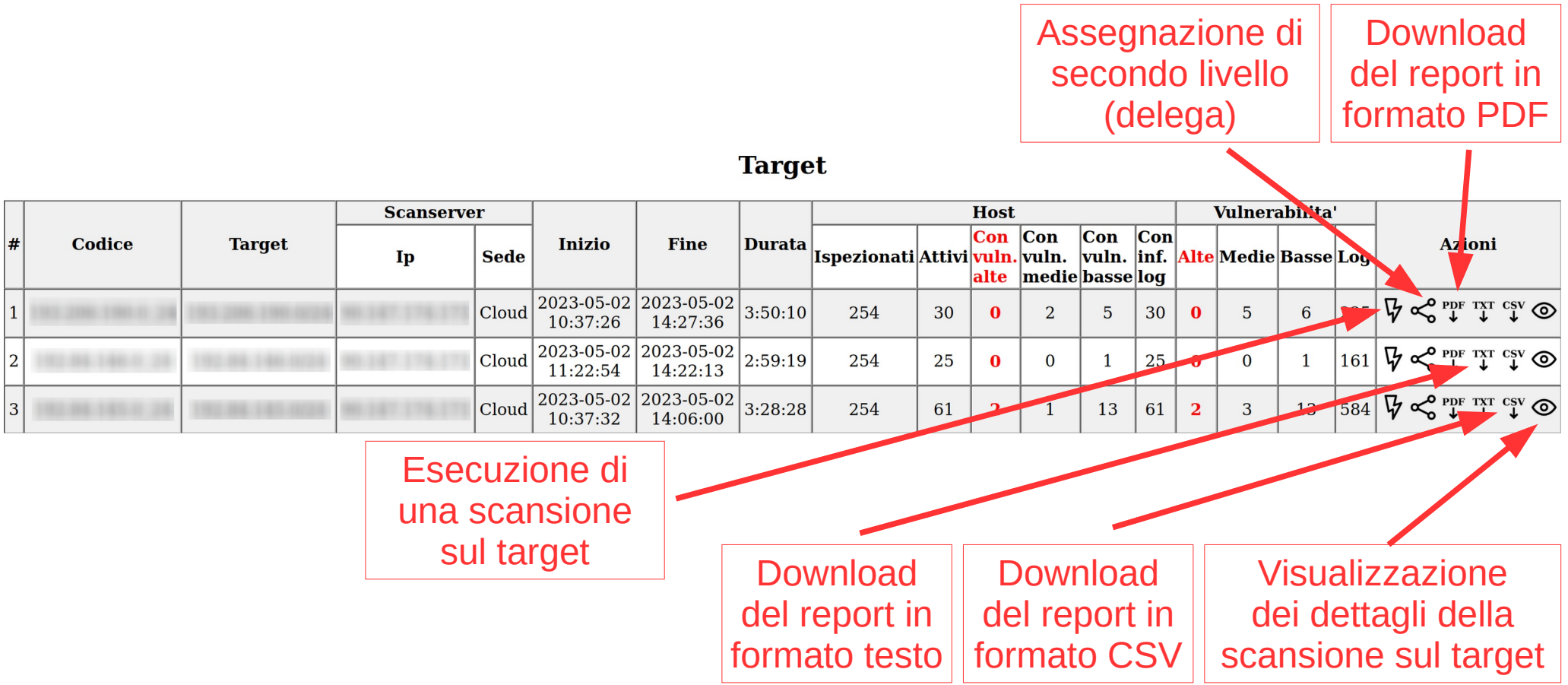
Consultazione e **gestione** di tutti gli host e le reti in carico

Consultazione e **gestione** delle deleghe di secondo livello

Risultati delle scansioni: target [1/3]



Risultati delle scansioni: target [2/3]



#	Codice	Target	Scanserver		Inizio	Fine	Durata	Host						Vulnerabilita'				Azioni
			Ip	Sede				Ispezionati	Attivi	Con vuln. alte	Con vuln. medie	Con vuln. basse	Con inf. log	Alte	Medie	Basse	Log	
1	[redacted]	[redacted]	[redacted]	Cloud	2023-05-02 10:37:26	2023-05-02 14:27:36	3:50:10	254	30	0	2	5	30	0	5	6	[redacted]	PDF TXT CSV
2	[redacted]	[redacted]	[redacted]	Cloud	2023-05-02 11:22:54	2023-05-02 14:22:13	2:59:19	254	25	0	0	1	25	0	0	1	161	PDF TXT CSV
3	[redacted]	[redacted]	[redacted]	Cloud	2023-05-02 10:37:32	2023-05-02 14:06:00	3:28:28	254	61	[redacted]	1	13	61	2	3	[redacted]	584	PDF TXT CSV

Risultati delle scansioni: target [3/3]

Target: [redacted]

Dettagli della scansione

Tipo: openvas
Data: 2023-05-20 08:57:33
Codice: 230502_01
Nome: POC_Firenze-alive_test-no_credentials
Descrizione: Scansione openvas dall'esterno sulla Sezione di Firezne con alive test
Durata: 3:50:10
Inizio: 2023-05-02 10:37:26
Fine: 2023-05-02 14:27:36

Dettagli del target

Codice del target: [redacted]
Target: [redacted]
Scanserver: [redacted]
Durata: 3:28:28
Inizio: 2023-05-02 10:37:32
Fine: 2023-05-02 14:06:00

Numero di host ispezionati: 254
Numero di host attivi: 61

Numero di host attivi con vulnerabilita' alte: 2
Numero di host attivi con vulnerabilita' medie: 1
Numero di host attivi con vulnerabilita' basse: 13
Numero di host attivi con informazioni (log): 61

Numero di vulnerabilita' gravi: 2
Numero di vulnerabilita' medie: 3
Numero di vulnerabilita' basse: 13
Numero di informazioni (log): 584

Host

Host

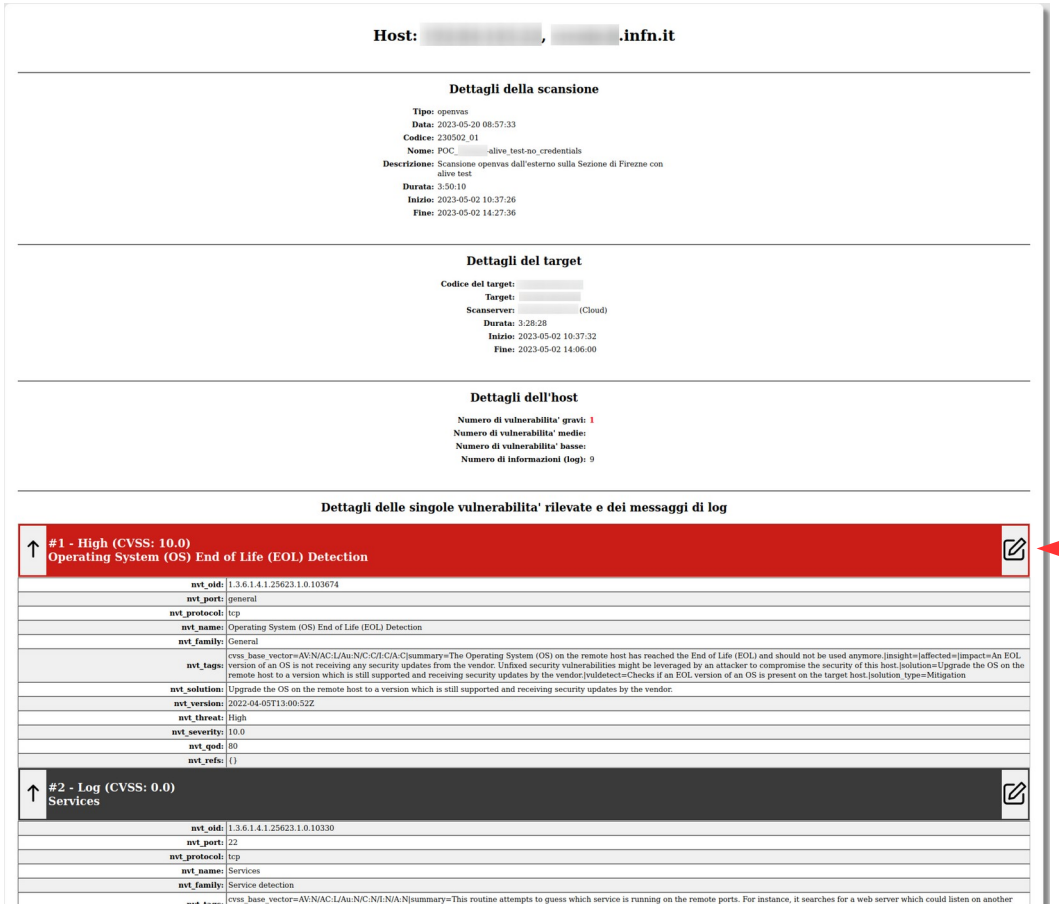
#	IP	FQDN	Vulnerabilita'				Azioni
			Alte	Medie	Basse	Log	
1	[redacted]	[redacted]				6	
2	[redacted]	[redacted]			1	101	
3	[redacted]	[redacted]				6	
4	[redacted]	[redacted]				6	
5	[redacted]	[redacted]				6	
6	[redacted]	[redacted]				6	
7	[redacted]	[redacted]			1	9	
8	[redacted]	[redacted]			1	20	
9	[redacted]	[redacted]			1	35	
10	[redacted]	[redacted]				6	
11	[redacted]	[redacted]				6	
12	[redacted]	[redacted]				6	
13	[redacted]	[redacted]			1	9	
14	[redacted]	[redacted]			1	7	
15	[redacted]	[redacted]				5	
16	[redacted]	[redacted]				6	
17	[redacted]	[redacted]				6	
18	[redacted]	[redacted]	1			9	
19	[redacted]	[redacted]				6	
20	[redacted]	[redacted]			1	20	
21	[redacted]	[redacted]				5	

Esegui una scansione sull'IP

Delega ad un altro utente la gestione dell'IP

Visualizza e **gestisci** le vulnerabilità dell'IP

Visualizzazione e gestione delle vulnerabilità [1/2]



Host: [redacted], [redacted].infn.it

Dettagli della scansione

Tipo: openvas
Data: 2023-05-20 08:57:33
Codice: 230502_01
Nome: POC_[redacted]alive_test-no_credentials
Descrizione: Scansione openvas dall'esterno sulla Sezione di Firenze con alive test
Durata: 3:50:10
Inizio: 2023-05-02 10:37:26
Fine: 2023-05-02 14:27:36

Dettagli del target

Codice del target: [redacted]
Target: [redacted]
Scanserver: [redacted] (Cloud)
Durata: 3:28:28
Inizio: 2023-05-02 10:37:32
Fine: 2023-05-02 14:06:00

Dettagli dell'host

Numero di vulnerabilita' gravi: 1
Numero di vulnerabilita' medie:
Numero di vulnerabilita' basse:
Numero di informazioni (log): 9

Dettagli delle singole vulnerabilita' rilevate e dei messaggi di log

#1 - High (CVSS: 10.0)
Operating System (OS) End of Life (EOL) Detection

nvt_oid:	1.3.6.1.4.1.25623.1.0.103674
nvt_port:	general
nvt_protocol:	tcp
nvt_name:	Operating System (OS) End of Life (EOL) Detection
nvt_family:	General
nvt_tags:	cvss_base_vector=AV:N/AC:L/Au:N/C:C/I:C/A:C|summary=The Operating System (OS) on the remote host has reached the End of Life (EOL) and should not be used anymore.|insight=|affected=|impact=An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.|solution=Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.|vuldetect=Checks if an EOL version of an OS is present on the target host.|solution_type=Mitigation
nvt_solution:	Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.
nvt_version:	2022-04-05T13:00:52Z
nvt_threat:	High
nvt_severity:	10.0
nvt_qod:	80
nvt_refs:	()

#2 - Log (CVSS: 0.0)
Services

nvt_oid:	1.3.6.1.4.1.25623.1.0.10330
nvt_port:	22
nvt_protocol:	tcp
nvt_name:	Services
nvt_family:	Service detection
	cvss_base_vector=AV:N/AC:L/Au:N/C:N/I:N/A:N|summary=This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another

Gestione della vulnerabilità

Visualizzazione e gestione delle vulnerabilità [2/2]

#	Data	Stato	vu fi
1	2023-05-02 10:45:28	nuovo	
2	2023-05-24 19:11:11	lavori in corso	
3	2023-05-24 19:11:55	risolto	
4	2023-05-24 19:13:40	lavori in corso	
5	2023-05-24 19:14:23	risolto	
6	**2023-05-24 19:16:30**		

- nuovo
- falso positivo
- lavori in corso
- non risolvibile

Dettaglio e gestione della vulnerabilita' o dei messaggi di log

[redacted], [redacted].infn.it

Dettaglio della singola vulnerabilita' rilevata o del messaggio di log

#1 - High (CVSS: 10.0)
Operating System (OS) End of Life (EOL) Detection

Rilevazione:	2023-05-02 10:45:28
nvt_oid:	1.3.6.1.4.1.25623.1.0.103674
nvt_port:	general
nvt_protocol:	tcp
nvt_name:	Operating System (OS) End of Life (EOL) Detection
nvt_family:	General
nvt_tags:	cvss_base_vector=AV:N/AC:L/Au:N/C:C/I:C/A:C|summary=The Operating System (OS) on the remote host has reached the End of Life (EOL) and should not be used anymore.|insight=|affected=|impact=An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.|solution=Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.|vuldetect=Checks if an EOL version of an OS is present on the target host.|solution_type=Mitigation
nvt_solution:	Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.
nvt_version:	2022-04-05T13:00:52Z
nvt_threat:	High
nvt_severity:	10.0
nvt_qod:	80
nvt_refs:	{}

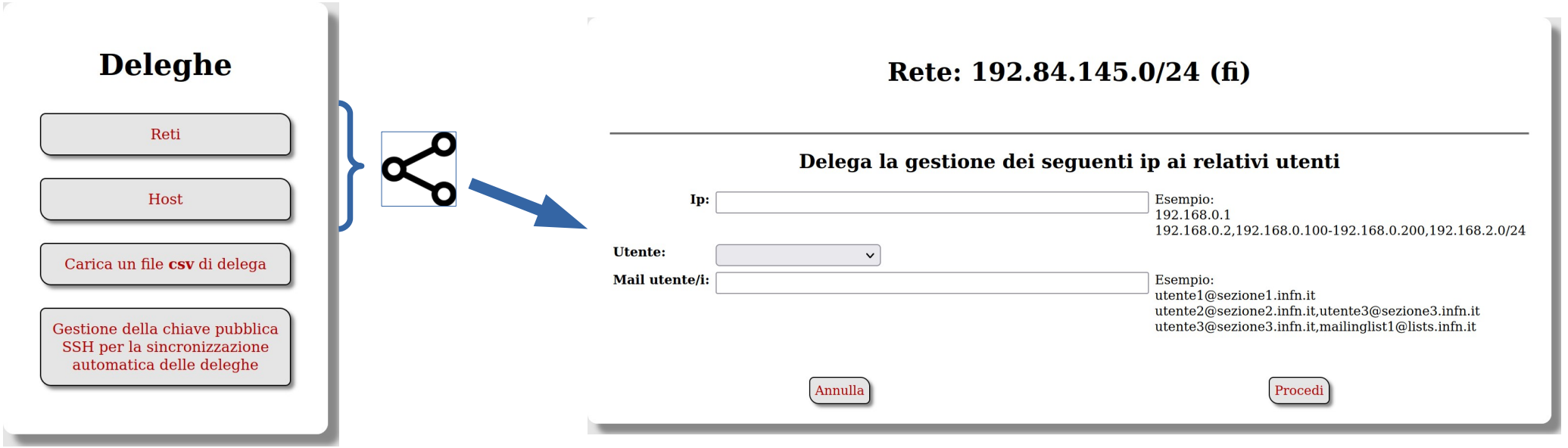
Gestione della singola vulnerabilita' rilevata o del messaggio di log

#	Data	Stato	Non segnalare questa vulnerabilita' fino alla data	Note	Utente	Azione
1	2023-05-02 10:45:28	nuovo				
2	2023-05-24 19:11:11	lavori in corso		Inizio a guardare di cosa si tratta	Leandro Lanzi	
3	2023-05-24 19:11:55	risolto		Ho aggiornato i pacchetti della distribuzione	Leandro Lanzi	
4	2023-05-24 19:13:40	lavori in corso		Non e' bastato aggiornare i pacchetti, devo aggiornare la distribuzione	Leandro Lanzi	
5	2023-05-24 19:14:23	risolto		Passato all'ultima versione del sistema operativo	Leandro Lanzi	
6	**2023-05-24 19:16:30**				Leandro Lanzi	

Deleghe (assegnazioni di secondo livello) [1/3]

- Sono previste 3 procedure per assegnare le deleghe nell'interfaccia web.

  1) Usando il pulsante  per scegliere gli IP o le reti e indicando gli utenti (tramite e-mail o scegliendo gli utenti già registrati da una lista).



Deleghe (assegnazioni di secondo livello) [2/3]

2) Caricando un file di testo nell'interfaccia web.

Carica un file csv di delega

Delega la gestione di ip e reti ai relativi utenti

Seleziona il file...

- (•) Aggiungi solo le nuove deleghe (lascia inalterate vecchie regole non modificate)
- ( ) Sostituisci tutte le deleghe (elimina le vecchie regole e sostituiscile con le nuove)

Caricare un file di testo **csv**.
Sono ammesse righe di commento utilizzando il carattere '#' (carattere 'cancelletto').
Come separatore delle colonne usare il carattere '|' (carattere 'pipe').
Nelle colonne riportare i seguenti dati:

- Elenco di singoli ip, reti o intervalli di ip - *obbligatorio*
  (es: 192.168.0.1, 192.168.0.0/24, 192.168.1.10-192.168.1.30)
- UID dell'utente INFN-AAI a cui assegnare la delega - *obbligatorio*
- Data di inizio della delega (formato: aaaa-mm-dd)
- Data di fine della delega (formato: aaaa-mm-dd)

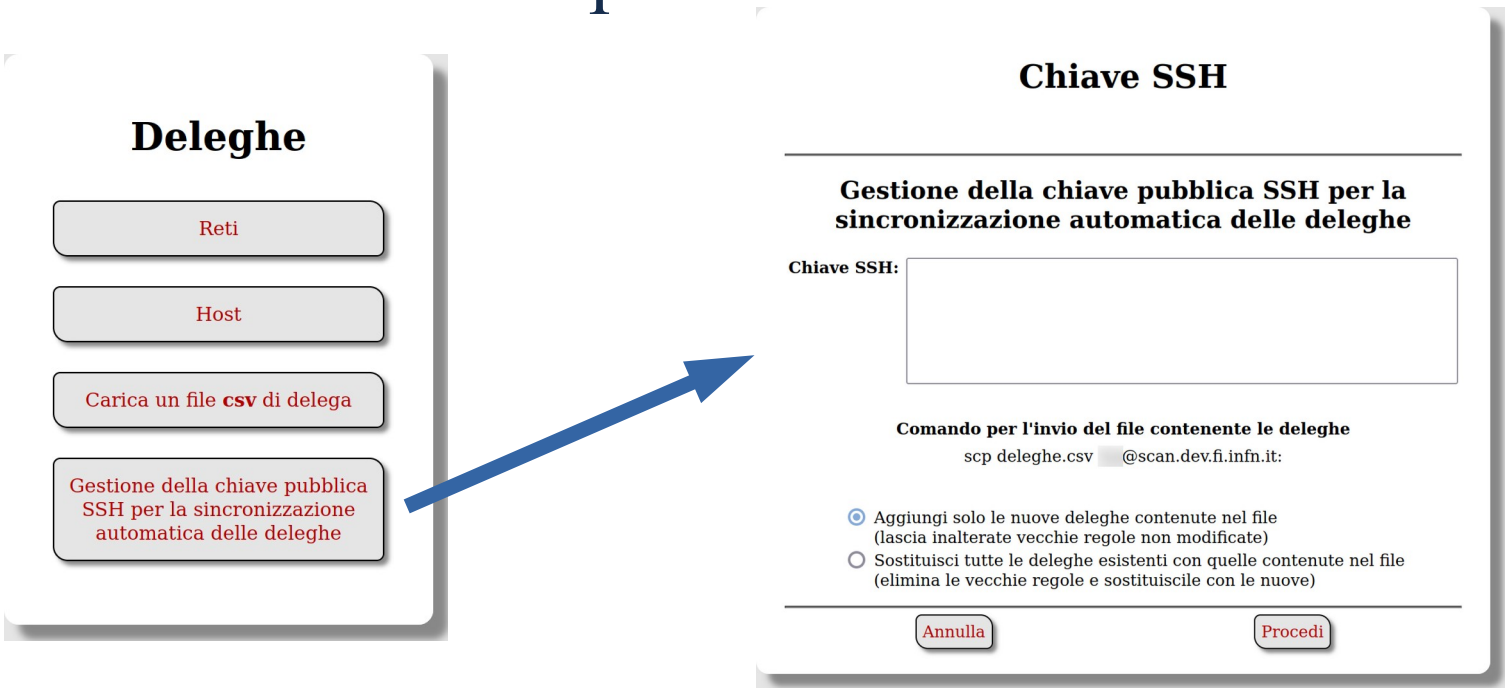
Esempio:

```
# Questo e' un file d'esempio
# ip/reti | INFN-AAI UID | Data inizio | Data fine
192.168.0.1|gino|2023-05-01|2023-12-31
192.168.0.2,192.168.0.3,192.168.0.4|pino|2023-05-01|2023-12-31
192.168.0.10-192.168.0.20|lino|2023-05-01|2023-12-31
192.168.0.0/24,192.168.1.0/24|nino|2023-05-01|2023-12-31
192.168.0.1,192.168.0.10-192.168.0.20,192.168.1.0/24,192.168.2.0/24|rino|2023-05-01|2023-12-31
```

Annulla Procedi

Deleghe (assegnazioni di secondo livello) [3/3]

3) Inviando tramite `scp` un file di testo al server web, dopo aver caricato la chiave pubblica SSH nell'interfaccia web.



Considerazioni finali

- Il lavoro non è concluso ma dovrebbe essere pronto per agosto (2023).
- La risoluzione dei problemi rilevati tramite le scansioni riguarderà direttamente chi amministra gli host vulnerabili quindi è necessaria la loro collaborazione.
- Questa interfaccia web ha come scopo:
  - quello di fornire agli amministratori di host vulnerabili uno strumento per conoscere quali sono i problemi rilevati e le operazioni da intraprendere per la loro soluzione ma anche per tener traccia del loro lavoro;
  - permettere di eseguire scansioni da parte degli amministratori (anche per verificare l'efficacia dei loro interventi);
  - coinvolgere solo chi è direttamente interessato alla soluzione dei problemi rilevati, liberando i Referenti della Sicurezza delle varie Sedi dall'onere di dover fare da tramite fra amministratori e NUCS, permettendo loro comunque di monitorare lo stato di avanzamento dei lavori.
- Le procedure di delega della gestione degli host ai diretti amministratori è stata pensata per essere compatibile ed integrabile in un eventuale futuro "database nazionale degli asset" in cui ogni host viene assegnato ad una o più persone fisiche.
- Dovrebbe poter essere utilizzato sia dalle varie Sedi che in ambito INFN-Cloud.
- Tutti i dati saranno accessibili agli Auditor GDPR.
- Devono essere implementate ancora le scansioni sui nomi host (FQDN, Fully Qualified Domain Name), oltre che sugli IP, ma il database è stato realizzato per tener conto di questa necessità: un host è identificato dalla coppia IP + nome host.
- Devono essere implementati ancora molti meccanismi di automazione e di avvisi automatici: in particolare il meccanismo che avvisa i Referenti della Sicurezza nel caso in cui gli amministratori di host vulnerabili trascurino le segnalazioni.
- Deve esser prodotto un documento che descriva la procedura di scansione e delle successive correzione delle vulnerabilità tramite questa interfaccia web oltre a descrivere il funzionamento dell'infrastruttura utilizzata per le scansioni.
- Deve esser prodotto un manuale per gli utenti dell'interfaccia web (servirà anche un corso di formazione?).
- Tutto il software utilizzato ed i sistemi operativi (GNU/Linux) di tutte le macchine dell'infrastruttura per le scansioni sono tutti open source e attualmente non viene pagata nessuna licenza.