Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

SCARR

Gianni Marzulli – GARR

Roma, 10/10/2019

Workshop GARR 2019

SCARR (**SCA**nsioni **R**ipetute a **R**ichiesta)

- Cosa è?

È un servizio (beta) di vulnerability scanning di criticità negli asset della rete GARR

  - basato su Greenbone (ex **OpenVAS)** e NMAP

- A chi è rivolto?

Agli **APM** GARR, per scansioni sulla propria rete di competenza

- What's new?

Servizio **self-service** fruibile autonomamente dall'utente via web

- Puntatori

https://scarr.garr.it

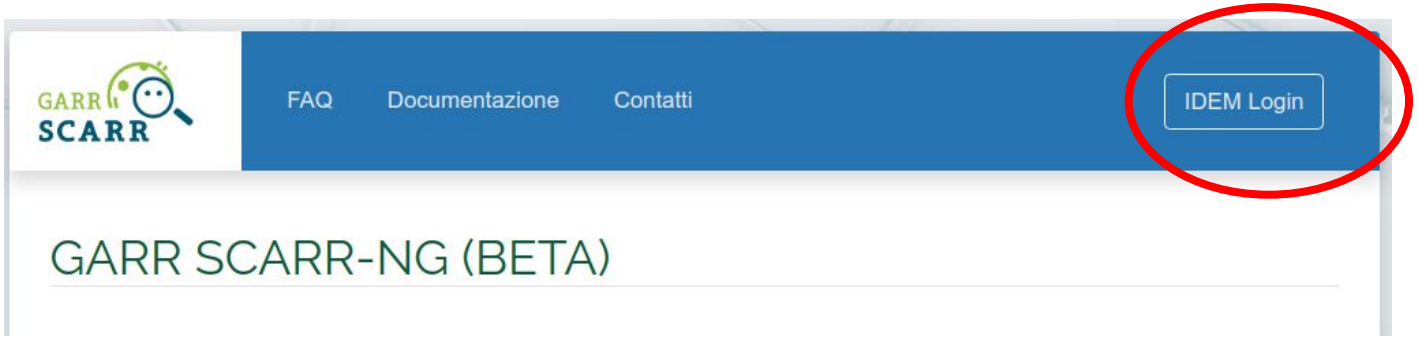
scarr-service@garr.it

Funzionalità

- Scansione di indirizzi IP
  - OpenVAS per classi C, NMAP per classi B
  - esecuzione asincrona e split delle richieste in task di scansione paralleli
- Advance scheduling con calendario e ripetibilità delle richieste
- Stato delle scansioni in corso in tempo reale e archivio di quelle terminate
- Report sulle vulnerabilità riscontrate, in ordine di criticità, con suggerimenti e indicazioni sulla mitigazione
  - notifiche e-mail

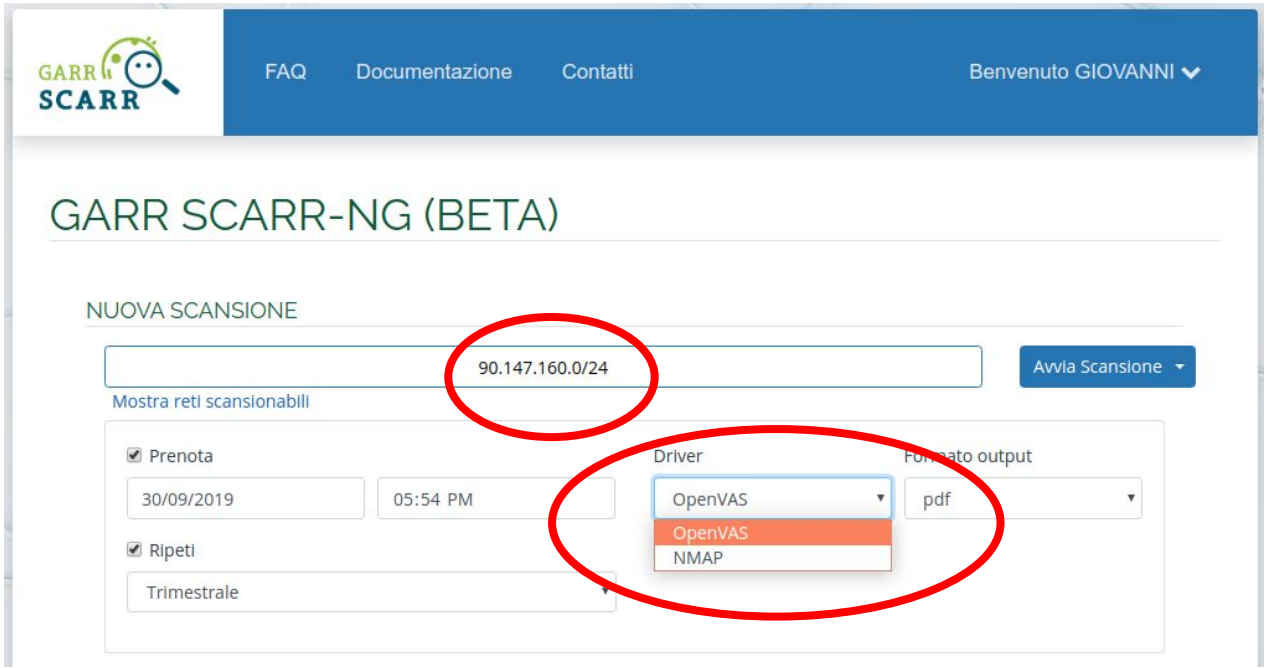
Come si usa - Login

- Autenticazione IDEM tramite il proprio account istituzionale
  - inizializzazione utente (creazione record nel database interno)
- Autorizzazione GARR-X DB
  - controlla che l'utente connesso sia un APM della rete GARR
  - assegna all'APM soltanto le reti di pertinenza della propria organizzazione, in modo che possa scansionare soltanto quelle



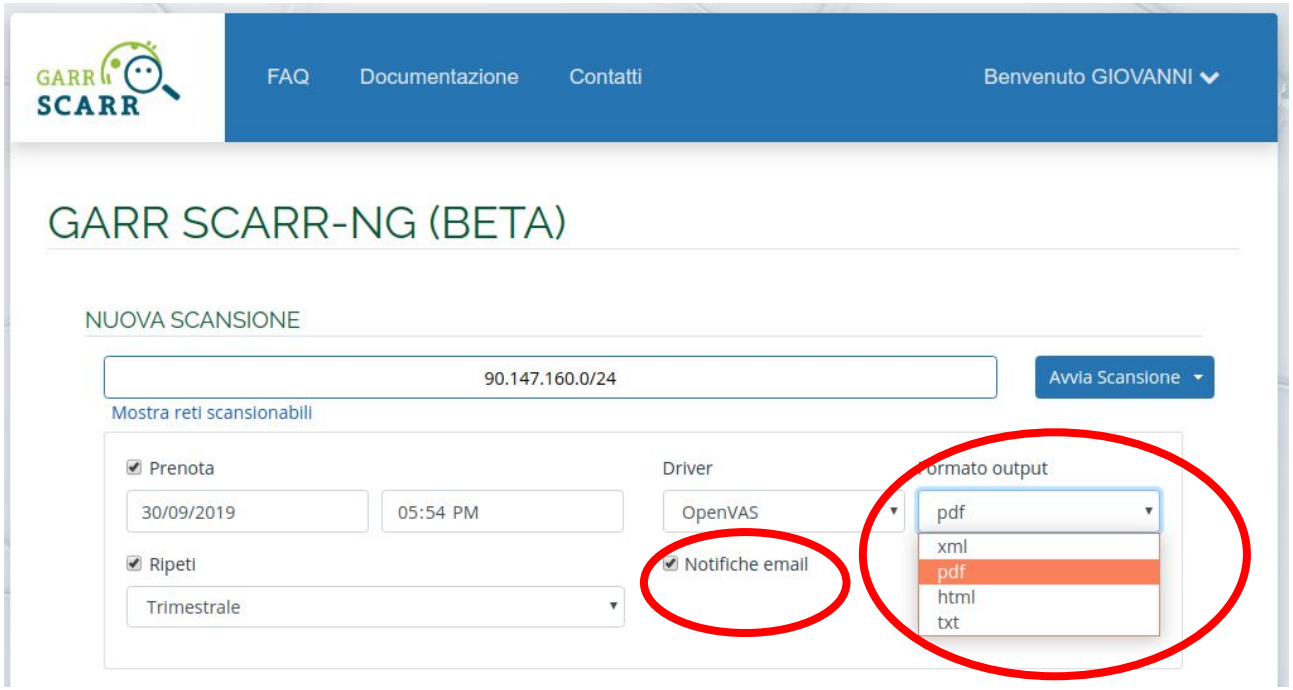
Come si usa - Nuova scansione

- Inserimento del target della scansione
  - singoli indirizzi IP, range e CIDR
  - scelta dello scanner OpenVAS o NMAP (beta)



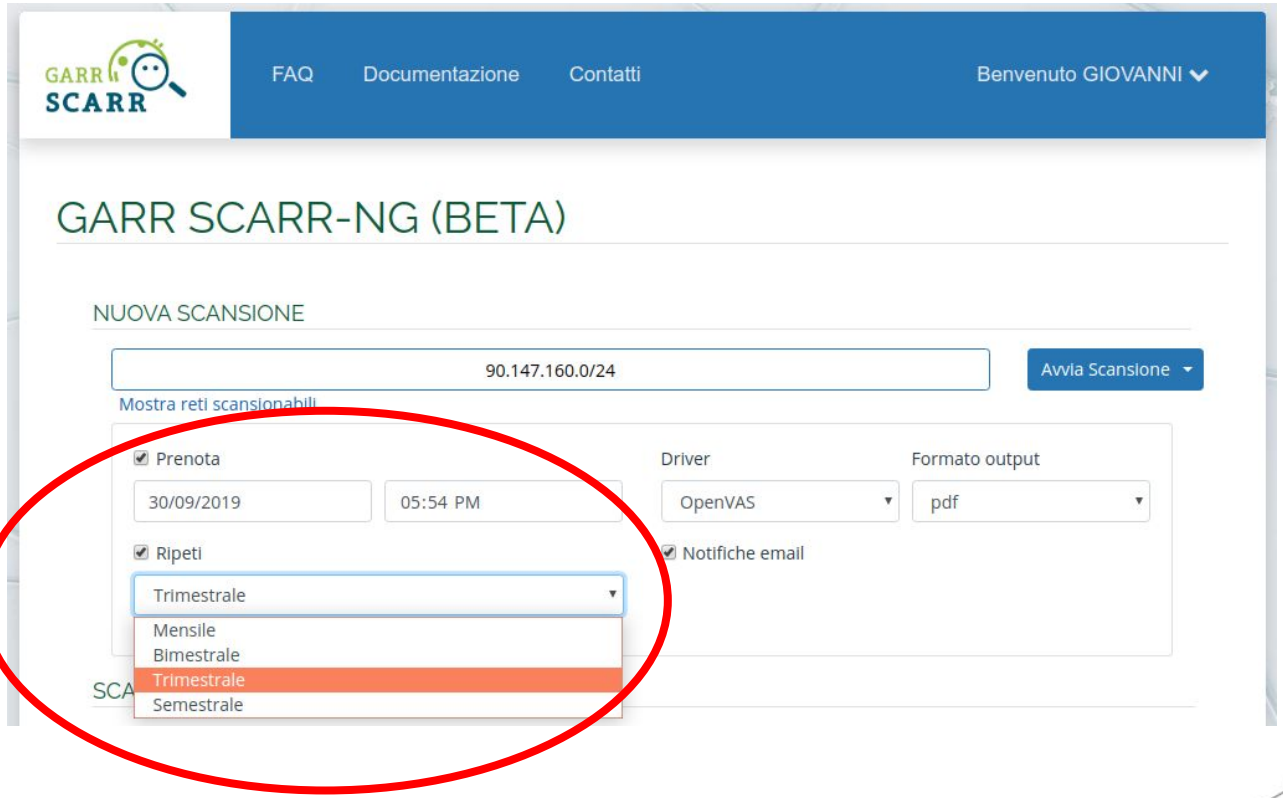
Come si usa - Nuova scansione

- Scelta del formato del report
  - PDF, HTML, XML, TXT



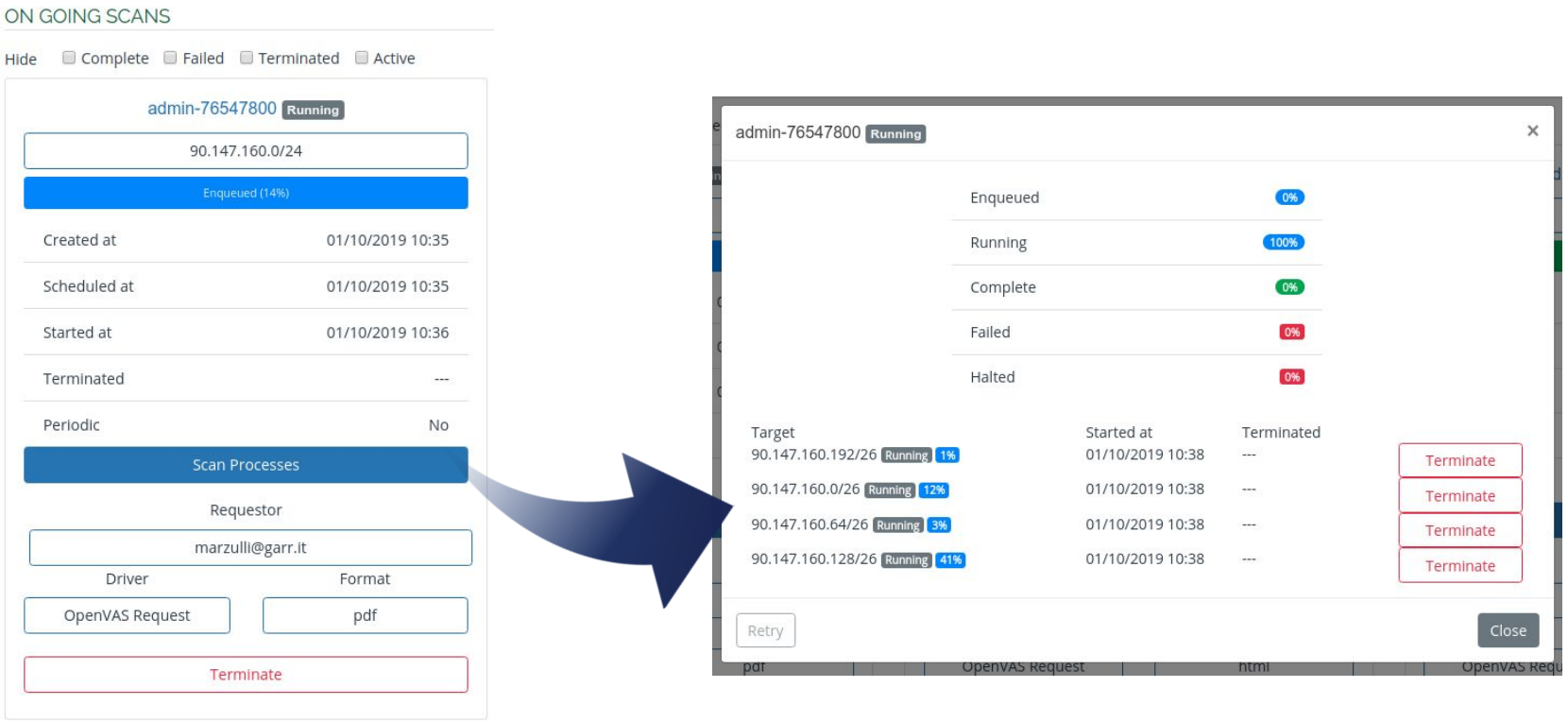
Come si usa - Nuova scansione

- Impostazione della prenotazione ad una certa data/ora desiderata
- Impostazione della ripetizione periodica



Come si usa - Stato della scansione

- Stato di avanzamento dei singoli sotto task



Come si usa - Report

Result Overview

Host	High	Medium	Low	Log	False Positive
90.147.90.177	0	3	0	16	0
Total: 1	0	3	0	16	0

Medium (CVSS: 4.3)
NVT: SSL/TLS: Report Weak Cipher Suites

Summary
This routine reports all Weak SSL/TLS cipher suites accepted by a service.
NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

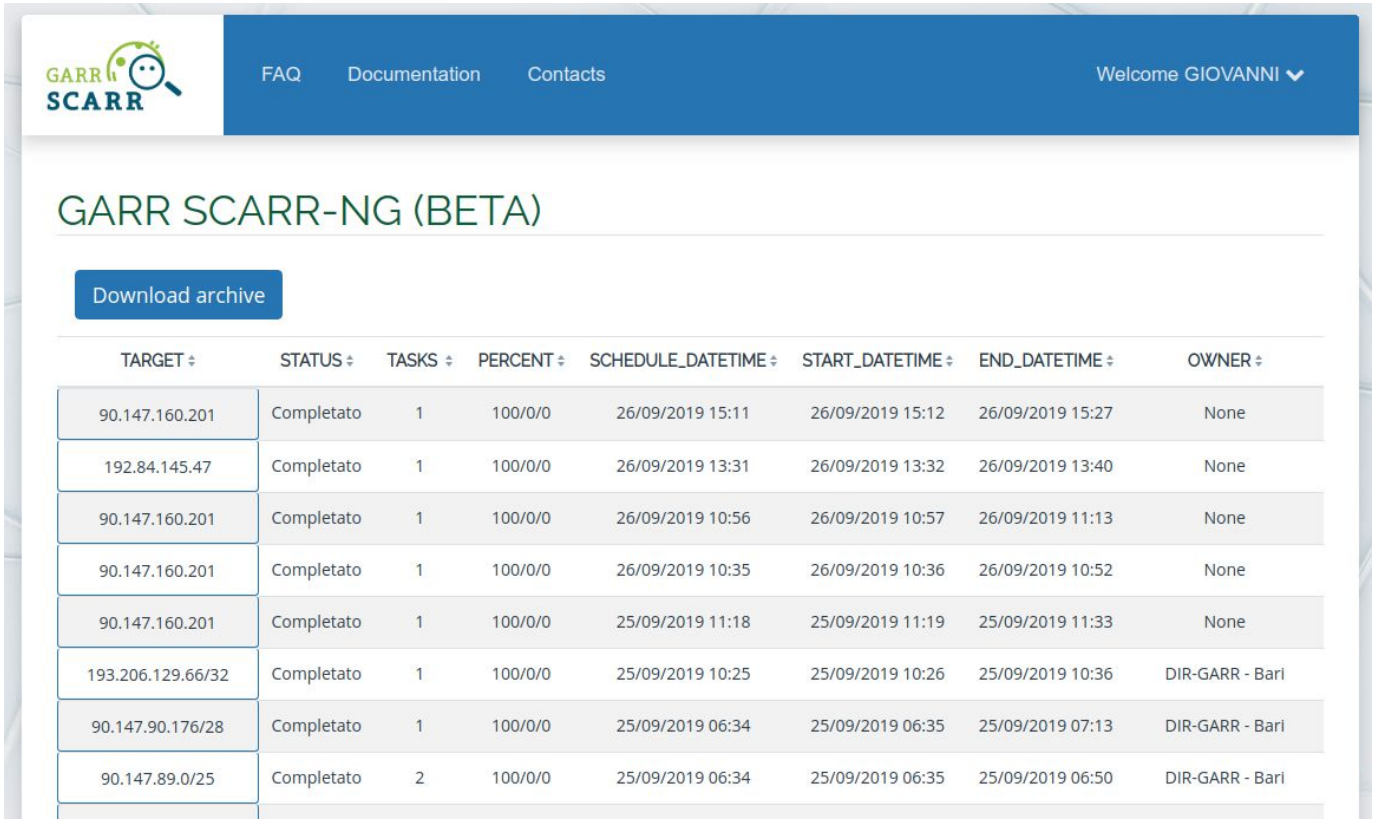
Vulnerability Detection Result
'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA

Solution
Solution type: Mitigation
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.

. . . continues on next page . . .

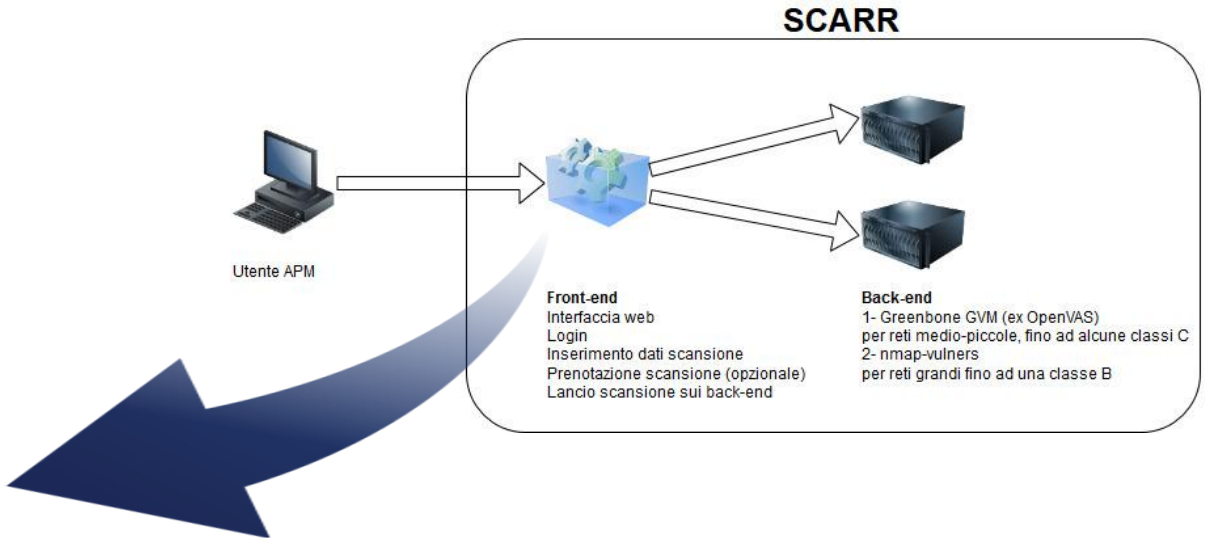
Come si usa - Archivio

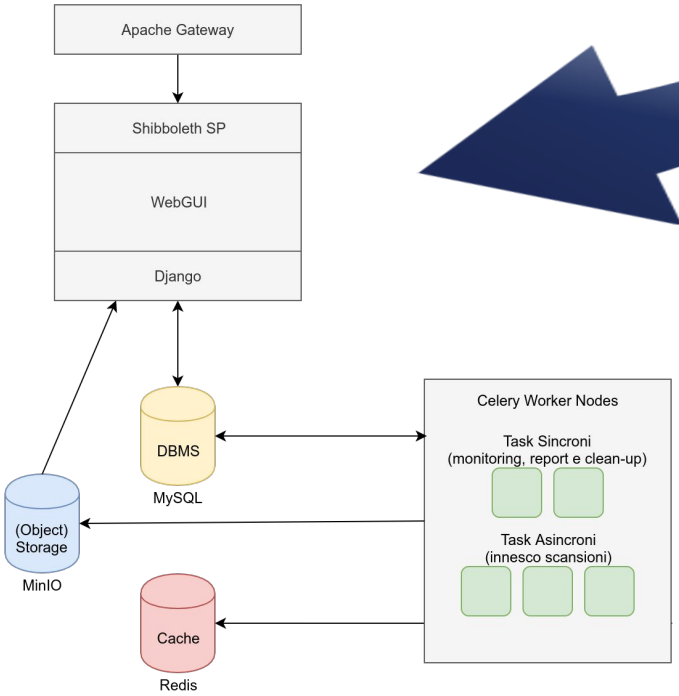
- Storico delle scansioni effettuate



TARGET	STATUS	TASKS	PERCENT	SCHEDULE_DATETIME	START_DATETIME	END_DATETIME	OWNER
90.147.160.201	Completato	1	100/0/0	26/09/2019 15:11	26/09/2019 15:12	26/09/2019 15:27	None
192.84.145.47	Completato	1	100/0/0	26/09/2019 13:31	26/09/2019 13:32	26/09/2019 13:40	None
90.147.160.201	Completato	1	100/0/0	26/09/2019 10:56	26/09/2019 10:57	26/09/2019 11:13	None
90.147.160.201	Completato	1	100/0/0	26/09/2019 10:35	26/09/2019 10:36	26/09/2019 10:52	None
90.147.160.201	Completato	1	100/0/0	25/09/2019 11:18	25/09/2019 11:19	25/09/2019 11:33	None
193.206.129.66/32	Completato	1	100/0/0	25/09/2019 10:25	25/09/2019 10:26	25/09/2019 10:36	DIR-GARR - Bari
90.147.90.176/28	Completato	1	100/0/0	25/09/2019 06:34	25/09/2019 06:35	25/09/2019 07:13	DIR-GARR - Bari
90.147.89.0/25	Completato	2	100/0/0	25/09/2019 06:34	25/09/2019 06:35	25/09/2019 06:50	DIR-GARR - Bari

Architettura





- Architettura a micro-servizi
  - applicazione multi-container basata su Docker
  - composizione e deployment tramite docker-compose

Conclusioni

- Nuovo servizio a disposizione della comunità, in beta aperta
  - self-service
- Sviluppi futuri
  - rilascio del driver per NMAP
  - scansioni di reti IPv6
  - reportistica avanzata (invio multiplo, merge, altri formati)
  - orchestrazione tramite Kubernetes

Grazie per l'attenzione