

SCARR

Gianni Marzulli - GARR

Roma, 10/10/2019

Workshop GARR 2019

SCARR (**SC**ansioni **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>

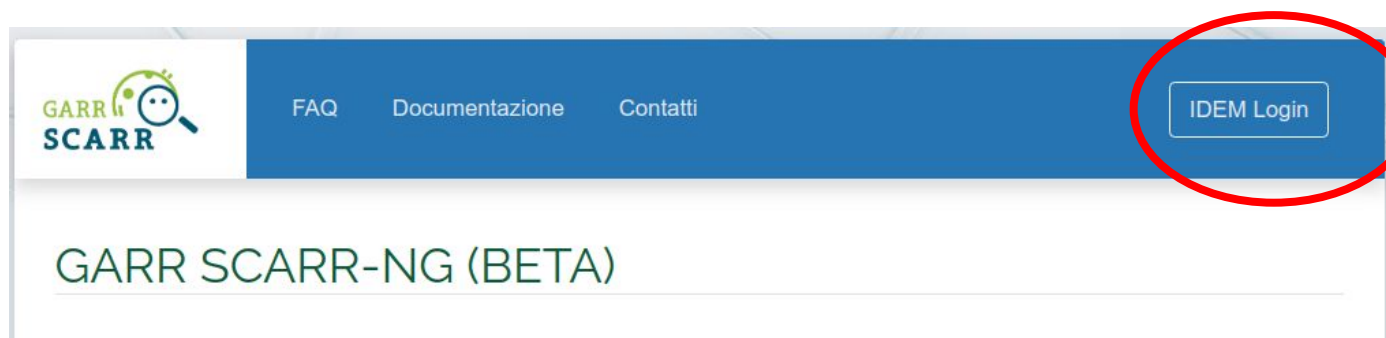
 scarr-service@garr.it



- 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

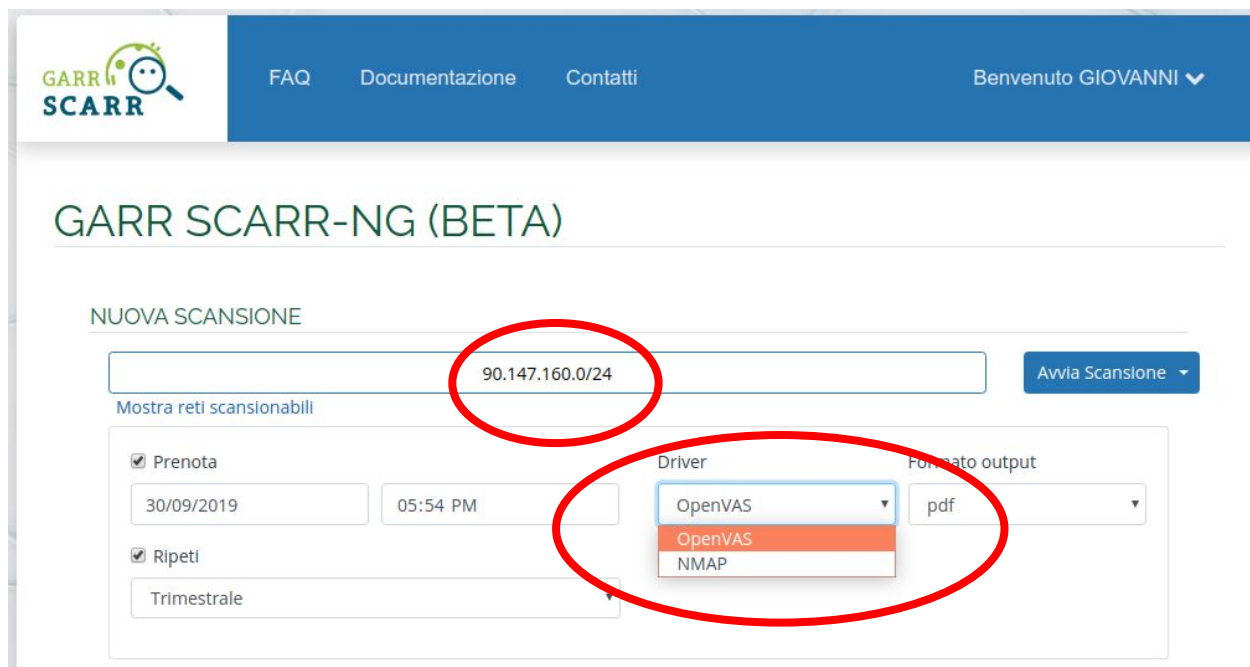
Come si usa - Login

- 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)



The screenshot shows the 'NUOVA SCANSIONE' (New Scan) form in the GARR SCARR-NG (BETA) application. The interface includes a top navigation bar with the GARR SCARR logo, links for FAQ, Documentazione, and Contatti, and a user greeting 'Benvenuto GIOVANNI'. The main form area is titled 'NUOVA SCANSIONE' and contains several input fields and a 'Avvia Scansione' button. A red circle highlights the target IP address '90.147.160.0/24' in the 'Target' field. Another red circle highlights the 'Driver' dropdown menu, which is open and shows 'OpenVAS' as the selected option, with 'OpenVAS' and 'NMAP' listed as available options. The 'Formato output' dropdown is set to 'pdf'. Other fields include 'Prenota' (30/09/2019, 05:54 PM), 'Ripeti' (Trimestrale), and 'Mostra reti scansionabili'.

Come si usa - Nuova scansione

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

GARR SCARR

FAQ Documentazione Contatti Benvenuto GIOVANNI ▼

GARR SCARR-NG (BETA)

NUOVA SCANSIONE

90.147.160.0/24 Avvia Scansione ▼

[Mostra reti scansionabili](#)

☒ Prenota
30/09/2019 05:54 PM

☒ Ripeti
Trimestrale ▼

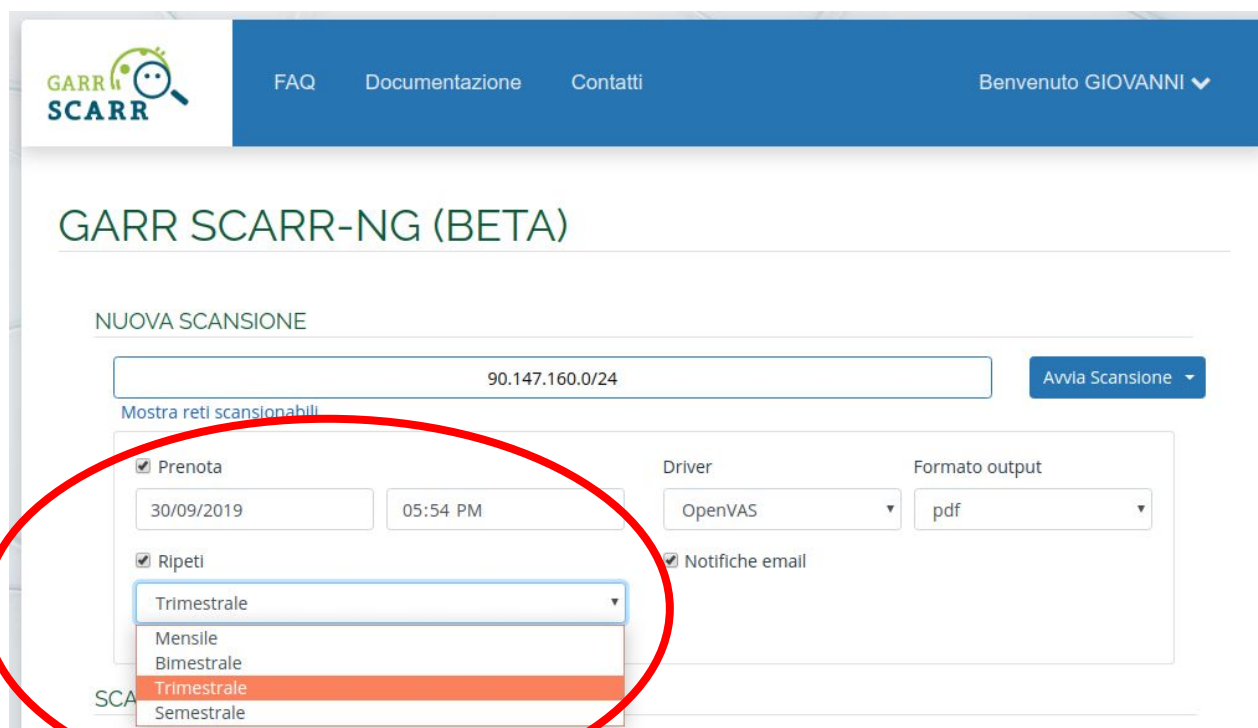
Driver
OpenVAS

☒ Notifiche email

Formato output
pdf
xml
pdf
html
txt

Come si usa - Nuova scansione

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



GARR SCARR

FAQ Documentazione Contatti Benvenuto GIOVANNI ▼

GARR SCARR-NG (BETA)

NUOVA SCANSIONE

90.147.160.0/24 Avvia Scansione ▼

Mostra reti scansionabili

☒ Prenota
30/09/2019 05:54 PM

☒ Ripeti
Trimestrale
Mensile
Bimestrale
Trimestrale
Semestrale

Driver: OpenVAS ▼ Formato output: pdf ▼

☒ Notifiche email

Come si usa - Stato della scansione

- Stato di avanzamento dei singoli sotto task

ON GOING SCANS

Hide ☐ Complete ☐ Failed ☐ Terminated ☐ Active

admin-76547800 **Running**

90.147.160.0/24

Enqueued (14%)

Created at 01/10/2019 10:35

Scheduled at 01/10/2019 10:35

Started at 01/10/2019 10:36

Terminated ---

Periodic No

Scan Processes

Requestor

marzulli@garr.it

Driver Format

OpenVAS Request pdf

Terminate

admin-76547800 **Running**

| | |
|----------|------|
| Enqueued | 0% |
| Running | 100% |
| Complete | 0% |
| Failed | 0% |
| Halted | 0% |

| Target | Started at | Terminated |
|--------------------------------------|------------------|------------|
| 90.147.160.192/26 Running 1% | 01/10/2019 10:38 | --- |
| 90.147.160.0/26 Running 12% | 01/10/2019 10:38 | --- |
| 90.147.160.64/26 Running 3% | 01/10/2019 10:38 | --- |
| 90.147.160.128/26 Running 41% | 01/10/2019 10:38 | --- |

Retry

Close

pdf OpenVAS Request html OpenVAS Request

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

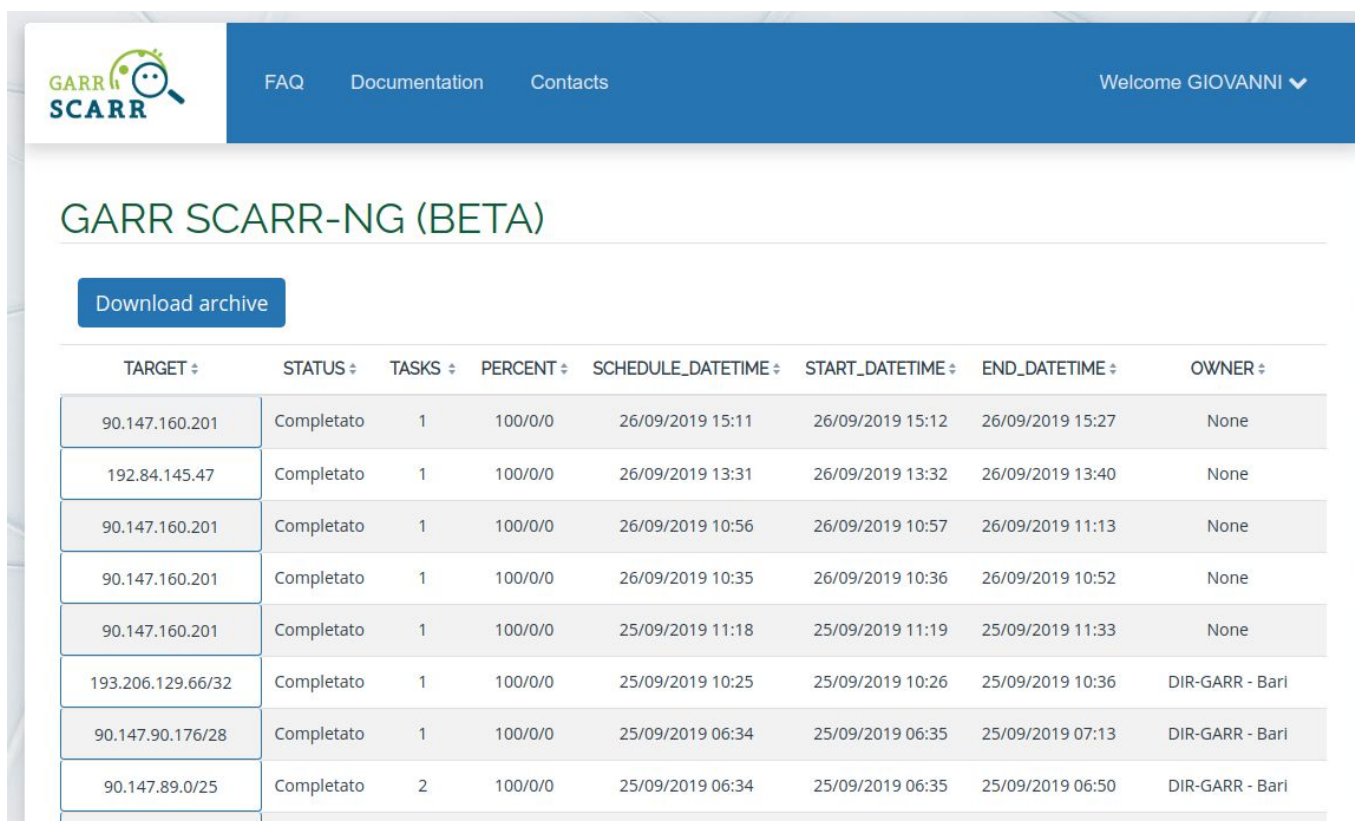
Solution

Solution type: Mitigation

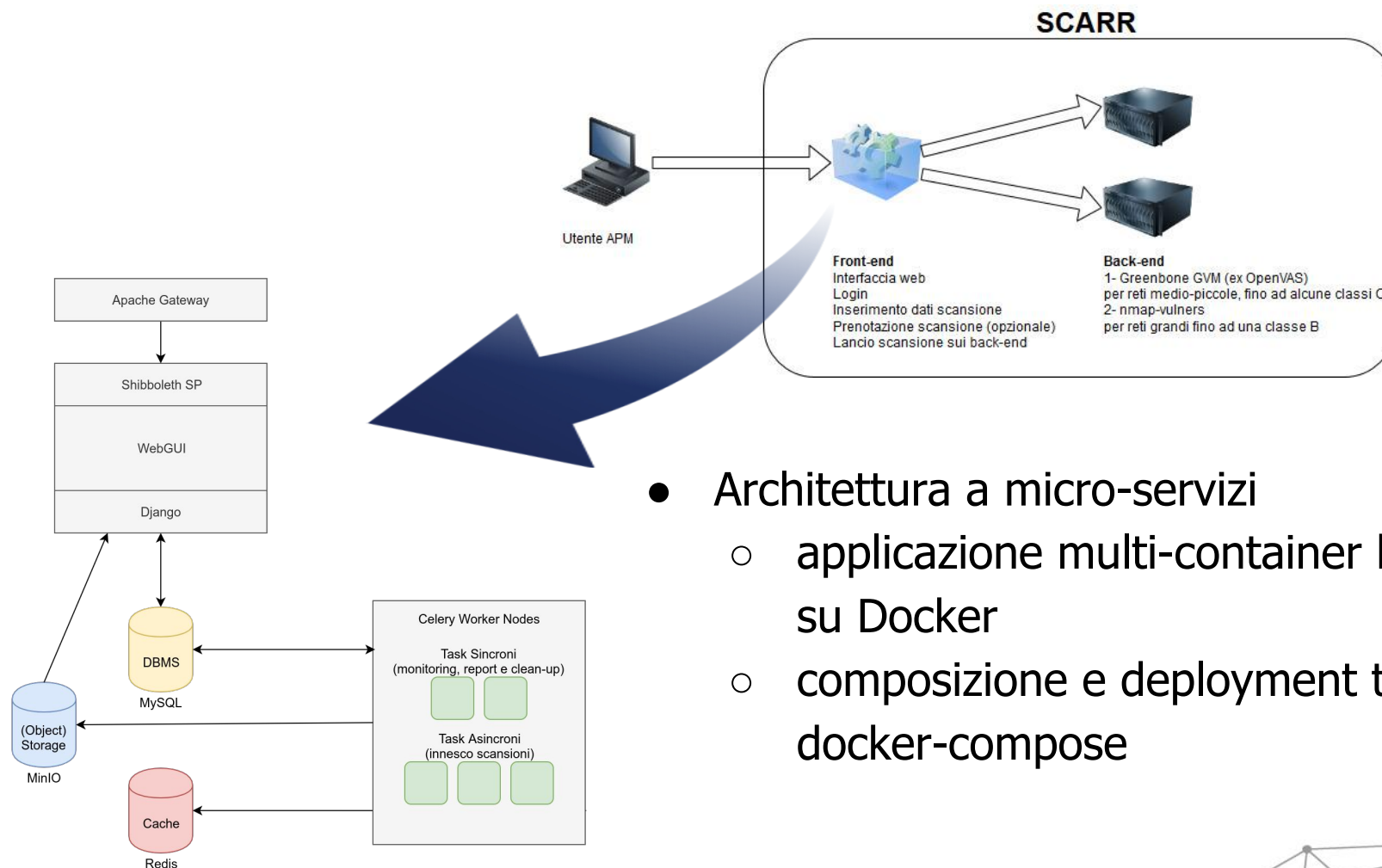
The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.

...continues on next page ...

- Storico delle scansioni effettuate

The screenshot shows the GARR SCARR-NG (BETA) web interface. At the top, there is a blue navigation bar with the GARR SCARR logo on the left, links for "FAQ", "Documentation", and "Contacts" in the center, and a "Welcome GIOVANNI" message with a dropdown arrow on the right. Below the navigation bar, the title "GARR SCARR-NG (BETA)" is displayed. A blue button labeled "Download archive" is positioned above a table. The table has eight columns: "TARGET", "STATUS", "TASKS", "PERCENT", "SCHEDULE_DATETIME", "START_DATETIME", "END_DATETIME", and "OWNER". It contains nine rows of data, all with a status of "Completato". The last three rows have an owner of "DIR-GARR - Bari".

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

- 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