Scansioni di sicurezza in INFN Cloud

Stefano Stalio

Miniworkshop sulla Sicurezza Informatica - Padova, 13-15 Febbraio 2023

Scansioni di sicurezza su INFN Cloud

Fin dal suo inizio della sua attività, INFN Cloud si è dotata di un **Security Incident Team** ed ha usato, tra gli altri, le scansioni di sicurezza come strumento per verificare e migliorare la sicurezza dei suoi servizi e di quelli realizzati dai suoi utenti

Nell'ottica della fondazione del nucleo di cybersecurity dell'INFN verrà descritto il lavoro fatto fino ad ora su INFN Cloud per quanto riguarda le scansioni di sicurezza

Scansioni: basate su Greenbone

INFN Datacloud usa l'**edizione community di Greenbone Security Assistant** come piattaforma per la gestione delle scansioni di sicurezza

Attualmente è **attiva la versione 21.4.3**, realizzata su una singola immagine docker (https://github.com/immauss/openvas)

Prevediamo di aggiornare alla versione più recente basandoci sul docker compose ufficiale di Greenbone dove i singoli servizi sono istanziati su container separati

Il docker-compose ufficiale è stato integrato con la **gestione automatica dei certificati Let's Encrypt via traefik** e con l'**aggiornamento periodico via cron del database delle vulnerabilità**.

https://baltig.infn.it/infn-cloud/greenbone-automation

Scansioni: 2 VM dedicate

Due VM, una a Bari ed una al CNAF, sull'infrastruttura Backbone di INFN Cloud, sono **dedicate alle scansioni di sicurezza**

Una delle due è attiva, la seconda può essere attivata in caso di necessità.

Alcuni degli host scansionati hanno regole di firewall che danno accesso alla porta 22 alle VM dedicate alle scansioni, per le scansioni autenticate

Al momento **circa 400 host scansionati** con frequenza bisettimanale

Punti fermi: regole ben chiare fin da subito

INFN Cloud è nata con delle regole ben definite riguardo all'utilizzo delle risorse IT da parte di utenti amministratori di sistema ed utenti semplici

A differenza di quello che spesso accade nelle sezioni INFN tutte le risorse attive su INFN Cloud sono state istanziate da persone ben consapevoli di queste regole e dei loro doveri e provviste di designazione ad amministratore di sistema

Punti fermi: ogni risorsa ha un amministratore

Ogni servizio o risorsa su INFN Cloud ha uno o più amministratori

Il meccanismo che gestisce le scansioni periodiche di sicurezza è in grado di associare ad ogni servizio o risorsa l’identità dei suoi amministratori

Punti fermi: INFN Cloud ha il controllo

Il team di INFN Cloud è tecnicamente in grado di isolare servizi/VM vulnerabili dalla rete ed ha procedure ben definite per farlo ed impedire all’utente di riattivare il servizio stesso

Punti fermi: per default tutto (o quasi) chiuso

Le VM istanziate su INFN Cloud con un IP pubblico espongono al mondo la porta 22 (ssh) e, **su esplicita azione dell'utente amministratore**, altre porte necessarie alla loro funzione specifica, ad esempio le porte 80 e la 443

Poiché solitamente le VM di INFN Cloud non rispondono al ping bisogna configurare Greenbone perché dia per scontato che i target definiti siano attivi e non si basi su un live test basato su ping

Punti fermi: sicurezza dei servizi PaaS/SaaS

Il livello di sicurezza dei servizi PaaS/SaaS offerti da INFN Cloud è verificato continuamente attraverso scansioni autenticate e con l'uso di strumenti di CI/CD

L'istanziazione di servizi di tipo PaaS che risultino soggetti a vulnerabilità viene sospesa fino a risoluzione del problema

Il SIT di INFN Cloud ha cura di trovare risoluzioni alle vulnerabilità riscontrate su servizi di tipo PaaS già attivi e di supportare gli utenti nell'applicarle

Scheduler esterno

Le scansioni periodiche di sicurezza non usano lo scheduler interno di Greenbone ma un semplice scheduler esterno:

- Limite sul numero degli host scansionati contemporaneamente (attualmente 2). In questo modo la VM che esegue Greenbone necessita di risorse limitate
- Lo scheduler privilegia nuovi target che non sono mai stati scansionati, poi accoda quelli già esistenti, ordinati a seconda della data dell'ultima scansione
- vengono scansionati i target per i quali l'ultima scansione è più "vecchia" di un intervallo minimo (attualmente 3 giorni)

Ridurre l’impatto delle scansioni

Allo scopo di ridurre l’impatto delle scansioni sui servizi sono stati presi i seguenti accorgimenti:

- Lo scheduler sottomette le **scansioni solamente in ore notturne**
- Il parallelismo dei test operati sull’host è limitato ad 1 (disabilitato)

Gestione automatizzata di target e task

Target e task sono creati ed eliminati in maniera automatica

Il meccanismo di automazione delle scansioni usa le API OpenStack per ottenere una lista sempre aggiornata delle VM in esecuzione sulle infrastrutture federate, con i relativi IP pubblici, i riferimenti degli amministratori ed altre informazioni di interesse per il supporto

Gestione automatizzata dei contatti

I riferimenti (nome ed e-mail) dell’amministratore o degli amministratori di ogni VM sono ricavati dai metadati associati alla VM stessa su OpenStack.

Scansioni sui nomi DNS

Il meccanismo di automazione delle scansioni accede al DNS di INFN Cloud via API ed ottiene i nomi DNS associati ad ogni indirizzo IP che deve essere scansionato. Il target Greenbone viene creato tenendo conto di tutti i nomi DNS associati all'indirizzo IP

Se un servizio istanziato via PaaS sfrutta nomi del tipo ***data.90.147.174.213.myip.cloud.infn.it***, non registrati in un DB DNS, tali nomi sono ricavati dai metadati associati alla VM su OpenStack. Anche questi nomi DNS sono associati al target openvas

La scansione per nome DNS è più efficace di quella per IP per quel che riguarda i servizi basati su http

Gestione automatizzata delle notifiche al SIT

Eventuali vulnerabilità sono notificate via mail al sistema di ticketing del SIT con tutte le informazioni necessarie, e col testo da inviare all'utente in caso si verifichi l'effettiva esistenza del problema

Notifiche all’utente

Il SIT di INFN Cloud inoltra le notifiche di vulnerabilità agli amministratori dei servizi una volta verificato

- Che la vulnerabilità esista effettivamente e che il servizio indicato ne sia effettivamente affetto
- Che la vulnerabilità sia risolvibile e che il SIT sia in grado di supportare l’utente nella sua risoluzione

Dear user,

You are the owner of a VM called minio-2 (ip address: 192.135.24.100 Lookup IP (https://trouble.cloud.inf
Add IP (https://trouble.cloud.infn.it/RTIR/Edit.html?id=2439&Object-RT::Ticket-2439-CustomField-10-AddVal
which is deployed on the INFN Cloud infrastructure.
During the latest security scan, a vulnerability scored 8.1/10 has been found.
Here the details:

- -----

Description:

The remote host is missing an update for the 'fail2ban' package(s) announced
via the USN-5232-1 advisory.
Jakub Zoczek discovered that certain Fail2ban actions handled whois responses
in
an insecure way. If Fail2ban was configured to use certain mail actions
like 'mail-whois' on a target system, a remote attacker who was able to control
whois
responses to this target system could possibly execute arbitrary code.

Solution:

Please install the updated package(s).

- -----

The whole report for your VM is attached to this message as a pdf file.

You are expected to solve this issue before March 26, 2023. Feel free to send
an e-mail to security@cloud.infn.it lookup email (https://trouble.cloud.infn.it/RTIR/Tools/Lookup.html?ti
lookup "cloud.infn.it" (https://trouble.cloud.infn.it/RTIR/Tools/Lookup.html?ticket=2439&type=host&q=clou
if you need help or advice on fixing this issue.

Gestione automatizzata delle scadenze temporali

Ad ogni vulnerabilità riscontrata da Greenbone è associata un valore numerico, da 1 a 10, che ne rappresenta la severità

A seconda della severità associata ad una vulnerabilità l'amministratore della risorsa ha una scadenza per la sua risoluzione

Nel caso la vulnerabilità non venga risolta in tempo, e dopo un ultimatum finale, la risorsa interessata viene spenta e all'utente viene negata la possibilità di riattivarla

Documentazione e supporto

Quando viene rilevata una nuova vulnerabilità, che riguarda più host o la cui risoluzione richiede procedure non ovvie ed in particolare quando la vulnerabilità si presenta su servizi istanziati dagli utenti attraverso la Dashboard PaaS di INFN Cloud, il SIT pubblica delle istruzioni per facilitare gli utenti nella risoluzione del problema
Il SIT di INFN Cloud è a disposizione degli utenti per supportarli nella risoluzione delle vulnerabilità riportate e per rispondere ad eventuali domande o dubbi

Fare login sulla macchina:

```
ssh username@IP_VM
```

E lanciare i seguenti comandi:

```
sudo -s

cd /usr/local/share/dodasts/jupyterhub
sed -i 's#dodasts/snj-base-jlabc:v1.0.*-snj#dodasts/snj-base-jlabc:v1.0.5-snj#'
docker-compose.yaml
docker-compose up -d
```

Supporto

Spesso gli utenti chiedono al SIT di verificare se le contromisure che hanno preso siano state efficaci nel risolvere le vulnerabilità riportate

Manca ad oggi **un meccanismo per rendere autonomo l'utente** nell'esecuzione di una scansione su un host da lei/lui gestito e nell'accedere al risultato

Scansioni autenticate

Tutte le macchine gestite da INFN Cloud e che offrono servizi sulla rete sono soggette a scansioni periodiche, alla stessa stregua delle VM degli utenti

In più su queste macchine esiste l'**utente non privilegiato "scans"** che Greenbone usa per accedere, attraverso una chiave SSH, all'oggetto della scansione ed eseguire dei controlli sul software installato, sul kernel in esecuzione, e su eventuali vulnerabilità correlate.

Scansioni come servizio

Le scansioni periodiche di sicurezza sulle VM istanziate dagli utenti rappresentano un **servizio** che viene offerto agli utenti stessi.

- Gli utenti di INFN Cloud hanno a disposizione delle istruzioni per la creazione dell'utente "**scans**" sulle loro VM e per il caricamento della corretta chiave pubblica.
- Se lo desiderano possono quindi far sì che le loro VM siano oggetto di scansioni più approfondite e non limitate ai soli servizi esposti al pubblico

Scansioni su immagini Docker

INFN Cloud offre ai suoi utenti un servizio di repository di immagini Docker basato su https://goharbor.io/

È possibile eseguire scansioni manuali o automatizzate sulle immagini Docker caricate

Turni e meeting

Il SIT di INFN Cloud si incontra (su Teams) ogni due settimane sul canale WP4 di INFN Datacloud

I ticket relativi alle vulnerabilità sono gestite da turnisti che fanno turni settimanali, dal lunedì al venerdì

Lessons learned

- Una gestione così granulare delle scansioni di sicurezza e delle vulnerabilità riscontrate richiede un effort notevole ed un impegno costante
- La garanzia dell'esistenza di un sistema simile rappresenta un valore aggiunto per i servizi di INFN Cloud e gli utenti ne sono consapevoli
- La sfida è trovare il modo di dare questo livello di servizio riducendo l'effort da parte di chi si occupa di sicurezza
- Sarebbe importante mettere in grado l'utente di eseguire scansioni in autonomia sulle proprie VM
- Servono meccanismi di automazione per quel che riguarda l'aggiornamento di VM e servizi istanziati attraverso la dashboard PaaS di INFN Cloud