Istituto Nazionale di Fisica Nucleare

NUcleo CyberSecurity

Scansioni di vulnerabilità

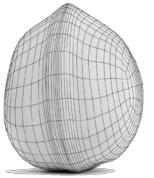
Gruppo scansioni del NUcleo di CyberSecurity dell'INFN

L. Lanzi, L. Carbone, V. Ciaschini, C. Greco, S. Stalio, G. Tagliente

Miniworkshop sulla Sicurezza Informatica

(Padova, 13-15 febbraio 2023)

Gruppo scansioni del NUCS (NUcleo CyberSecurity INFN)



- Partecipanti al gruppo:
  - Luca Carbone, *Milano Bicocca*
  - Vincenzo Ciaschini, *CNAF*
  - Cristian Greco, *Roma 2*
  - Leandro Lanzi, *Firenze* (coordinatore)
  - Gabriele Lo Re, *Pisa*
  - Vincenzo Spinoso, *Bari*
  - Stefano Stalio, *Laboratori Nazionali del Gran Sasso*
  - Gabriele Tagliente, *Laboratori Nazionali del Gran Sasso*
- Il gruppo si è formato a novembre 2022.
- 5 riunioni.

Obiettivi generali del gruppo

- Armonizzare l'attività delle scansioni di vulnerabilità in ambito CCR ed in ambito INFN-Cloud per arrivare ad una sintesi applicabile all'intera rete INFN che tenga conto dei punti di forza e delle criticità emerse dall'esperienza nei due ambiti.
- Rendere il più possibile automatici tutti i processi
  - di scansione,
  - di segnalazione delle vulnerabilità agli interessati,
  - di correzione delle vulnerabilità, cioè la segnalazione di:
    - falsi positivi,
    - risoluzione delle vulnerabilità (almeno quelle gravi),
    - impossibilità alla soluzione dei problemi,
    - ecc.
- Fornire uno strumento per creare e mantenere aggiornato un archivio degli amministratori di sistema dei singoli IP o di classi di IP.
- Mettere a disposizione di tutti
  - documentazione,
  - strumenti per compiere scansioni.
- Pubblicare costantemente e rendere accessibili tutti risultati delle scansioni vulnerabilità nella rete INFN.

Punti di forza e criticità emerse nella gestione delle scansioni in ambito INFN-Cloud

- **Punti di forza**
  - Automatismo in (quasi) tutto il processo di rilevamento, segnalazione e gestione della risoluzione delle vulnerabilità.
  - Conoscenza a priori di tutti i dati relativi alle risorse oggetto di scansioni: in particolare INFN-Cloud conosce chi è l'amministratore del singolo IP su cui vengono rilevate le vulnerabilità.
  - Interazione diretta con l'amministratore dell'IP vulnerabile.
  - Possibilità di *enforcing* da parte di INFN-Cloud: se la vulnerabilità non viene risolta nei tempi stabiliti, l'IP viene chiuso.
- **Criticità**
  - Impegno costante da parte del *security group* nel valutare i falsi positivi e, talvolta, particolarmente pesante nel fornire le indicazioni gli utenti per risolvere le vulnerabilità rilevate.

Punti di forza e criticità emerse nella gestione delle scansioni in ambito CCR

- **Punti di forza**
  - Automatismo nella rilevazione e nella pubblicazione delle vulnerabilità.
  - Permessi di accesso ai risultati delle scansioni gestite in base a **ruoli** impostati in INFN-AAI non a **nomi**. Il Responsabile del Servizio Calcolo e Reti di ogni struttura può definire i permessi di accesso a tutti i dati (in base a ruoli o nomi) che per default sono i seguenti:
    - gli afferenti al Servizio Calcolo e Reti di una struttura possono accedere a tutti i dati per quella struttura e definire un ulteriore gruppo di utenti (per ruolo o per nomi) che hanno accesso ai dati, sempre relativamente alla propria struttura.
- **Criticità**
  - Mancanza di conoscenza di chi sia l'amministratore reale del singolo IP su cui viene rilevata la vulnerabilità.
  - Impossibilità di seguire in modo capillare il processo di risoluzione delle singole vulnerabilità rilevate sui singoli IP.
  - Nessuna possibilità di *enforcing* nel caso in cui le vulnerabilità, per quanto gravi, non vengano risolte.

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.

Modello di gestione delle vulnerabilità (gravi) [1/2]

- In generale ogni scansione produce un report con l'elenco di tutte le vulnerabilità per ogni singolo IP.
- Per ora ci si limita a considerare solo le vulnerabilità gravi.
- Il livello di dettaglio necessario a INFN-Cloud per gestire le vulnerabilità prevede di **assegnare le singole vulnerabilità rilevate sul singolo IP all'amministratore di tale IP**, ma questa informazione non è quasi mai nota a livello nazionale.
- Per risolvere questo problema si propone un nuovo modello di gestione, esposto nel dettaglio nelle prossime pagine, che prevede di realizzare uno strumento per
  - la rilevazione,
  - la segnalazione,
  - la gestione e il monitoraggio delle correzioni

  delle vulnerabilità.

Modello di gestione delle vulnerabilità (gravi) [2/2]

- Tale strumento sarà messo a disposizione delle varie Strutture (Sezioni, Laboratori, Gruppi Collegati, Sistema Informativo, INFN-Cloud, ...) che potranno scegliere come usarlo.
- Tale strumento non implementerà nessun meccanismo per obbligare la risoluzione delle vulnerabilità in tempi certi o per richiedere priorità nella risoluzione di particolari vulnerabilità.
- Ogni struttura:
  - può definire uno o più ***Referenti*** (amministratori di sistema) per ogni singolo IP;
  - può organizzare i propri IP definendo dei ***Gruppi di IP***;
  - può definire uno o più *Referenti* per ogni *Gruppo di IP*.
- Ogni *IP* può appartenere a più *Gruppi di IP* e avere più *Referenti*.

Autenticazione ed autorizzazione

- L'autenticazione viene gestita tramite INFN-AAI.
- I **permessi di accesso ai risultati delle scansioni delle singole strutture vengono gestiti in INFN-AAI** in base a **ruoli** o a **nomi**.
- Gli afferenti a ciascuna struttura potranno accedere solo ai dati della propria struttura secondo il seguente schema.
  - ***Responsabile*** - Il Responsabile del Servizio Calcolo e Reti di ogni struttura (o figura equivalente) può definire i permessi di accesso a tutti i dati della propria struttura in base a ruoli o nomi. In particolare può definire il gruppo degli *Amministratori* e degli *Utenti*.
  - ***Amministratori*** - Per default sono gli afferenti al Servizio Calcolo e Reti di una Struttura (o figure equivalenti) e, otre a poter accedere a tutti i dati per quella struttura, possono definire un gruppo di U*tenti* (per ruolo o per nomi) in modo che questi abbiano accesso ai dati della propria struttura. Questa configurazione può essere comunque modificata dal *Responsabile* che può identificare *Amministratori* diversi.
  - ***Utenti*** - Gli utenti abilitati dagli *Amministratori* o dal *Responsabile* accedono ai dati ma non possono modificare i permessi di accesso.
- Questo schema di accesso permette, per esempio, ad un dipendente di una generica Struttura A di accedere ai dati di una Struttura B: il responsabile della Struttura B deve assegnargli il ruolo di *Amministratore* o di *Utente* per la sua struttura.
- L'accesso “fine”, del singolo *Referente* al singolo IP o al *Gruppo di IP* che amministra, viene gestito all'interno della piattaforma, non in INFN-AAI.

Rilevazione delle vulnerabilità

- Scansioni a ciclo continuo con **`nmpa`** e **`zmap`** su tutte le reti del domininio `infn.it`. al fine di identificare un ristretto numero di IP attivi.
  - Il livello di dettaglio dei risultati è:

    IP - Protocollo (TCP/UDP) - Porta
- Scansioni con **Greenbone Community Edition (GCE)**, spesso chiamato anche OpenVAS, solo sugli IP risultati attivi nelle scansioni `nmap`/`zmap` degli ultimi mesi.
  - Il livello di dettaglio dei risultati è:

    IP - Protocollo (TCP/UDP) - Porta - Vulnerabilità

Segnalazione delle vulnerabilità

- I risultati delle scansioni `nmpa` e `zmap` non vengono comunicati esplicitamente ma i dati saranno comunque consultabili via interfaccia web.
- I risultati delle scansioni con GCE vengono comunicati esplicitamente agli interessati secondo il seguente schema.
  - Se esiste uno o più *Referenti* dell'IP su cui viene rilevata la vulnerabilità vengono direttamente informati via mail.
  - Se non esiste il *Referente* del singolo IP ma l'IP fa parte di un *Gruppo di IP*, la segnalazione via mail viene inviata al *Referente* o ai *Referenti* del *Gruppo di IP*.
  - Ogni *Referente* riceverà una singola mail per tutti gli IP vulnerabili che amministra.
  - Se non esiste nessun *Referente* dell'IP su cui viene rilevata la vulnerabilità e l'IP non fa parte di nessun *Gruppo di IP*, la segnalazione via mail viene inviata all'APM GARR della rete di cui fa parte o al *Referente locale per la sicurezza informatica* (vedi pagina successiva).
  - Anche l'APM GARR o *Referente locale per la sicurezza informatica* riceveranno una singola mail per tutti gli IP vulnerabili della propria rete.

Referente locale per la sicurezza informatica

- In accordo col Nucleo di Cybersecurity dell'INFN, si ritiene utile identificare in ogni Sede (Sezione, Laboratorio, Gruppo collegato, ...) un unico **Referente locale per la sicurezza informatica** nominato dal Direttore della struttura, o al massimo un paio di persone (per il backup, ma non una mailing list), che abbia il compito, per quanto riguarda le scansioni di vulnerabilità, di **coordinare le operazioni di correzione delle vulnerabilità e di individuare gli amministratori di sistema degli IP risultati vulnerabili**.

Gestione e correzione delle vulnerabilità [1/3]

- Se la mail di segnalazione delle vulnerabilità arriva all'APM GARR o al *Referente locale per la sicurezza informatica* vuol dire che per gli IP oggetto della mail non sono stati definiti i *Referenti* (amministratori di sistema).

  Accedendo all'interfaccia web l'APM GARR o il *Referente locale per la sicurezza informatica* potrà

  - definire i *Referenti* degli IP segnalati,
  - oppure gestire le vulnerabilità direttamente.

Gestione e correzione delle vulnerabilità [2/3]

- Per ogni singola vulnerabilità per ogni singolo IP sono previste le seguenti azioni da parte del Referente dell'IP, dell'APM GARR o del *Referente locale per la sicurezza informatica*.
  - Conferma di ricezione
  - Apertura dell'attività di correzione.
  - Chiusura dell'attività di correzione:
    - segnalazione di un falso positivo;
    - segnalazione di risoluzione della vulnerabilità;
    - segnalazione eccezionale di impossibilità temporanea alla risoluzione della vulnerabilità (indicando un tempo massimo di risoluzione).
  - Tutte le azioni possono esser fatte
    - sulla singola vulnerabilità,
    - cumulativamente su tutte le vulnerabilità di un singolo IP,
    - cumulativamente su tutte le vulnerabilità di un gruppo IP,
    - cumulativamente su tutte le vulnerabilità di tutti gli IP della struttura.
  - Ci si aspetta che almeno la prima azione di “Conferma della ricezione” venga sempre effettuata da tutti gli interessati.

Gestione e correzione delle vulnerabilità [2/3]

- Ci si aspetta che almeno la prima azione di “Conferma della ricezione” venga sempre effettuata da parte di tutti gli interessati.
- In base al modo con cui vengono chiuse le attività di correzione per le varie vulnerabilità (falso positivo, risoluzione, ...), nelle successive scansioni verranno evitate segnalazioni ridondanti per problemi già risolti.
- Verrà mantenuto il sistema di ticket ma solo per uso interno del gruppo scansioni ed eventualmente per comunicare con gli utenti o gestire casi particolari.

  Gli utenti delle strutture non avranno accesso al sistema di ticket.

  Tutte le operazioni effettuate nell'interfaccia web verranno salvate automaticamente all'interno del sistema di ticket per semplificarne la consultazione dello storico da parte del gruppo scansioni.

Documentazione

- Abbiamo iniziato a raccogliere documentazione e how-to riguardanti le scansioni di vulnerabilità per metterli presto a disposizione di tutti.
  - È già pronta la documentazione per l'installazione nella propria infrastruttura o su INFN-Cloud di Greenbone Community Edition vers. 22.4 (la 21.4 è obsoleta da circa un mese) per chi vuole effettuare scansioni in proprio dall'interno o dall'esterno della propria rete.

Strumenti

- Abbiamo iniziato a raccogliere software (anche scritto da colleghi esterni al gruppo) per metterlo presto a disposizione di tutti.
  - Script forniti da Massimo Pistoni (LNF) per l'automatizzazione della configurazione di Greenbone Community Edition.

Contatti e materiale

- Per comunicare con il gruppo e per accedere a documentazione, strumenti e alla futura piattaforma di gestione delle scansioni una unica URL

  https://scan.fi.infn.it

  dalla quale si potrà accedere a tutto il resto.