Trivy vs Snyk

Confronto tra due scanner di vulnerabilità per container

Giovanni Bellini
Matricola: 600035
ICT Risk Assessment
Corso di laurea magistrale in Informatica
Università degli Studi di Pisa

Febbraio 2024

Indice

1 Introduzione **3**
1.1 Processo di scansione 3
1.1.1 Trivy 3
1.1.2 Snyk 4

2 Confronto **6**
2.1 Scansione delle vulnerabilità 6
2.2 Scansione di configurazioni IaC 7
2.3 Differenze di funzionalità 7
2.3.1 Trivy: scansione di cluster Kubernetes 7
2.3.2 Trivy: Scansione delle Configurazioni Infrastructure as Code (IaC) . . 8
2.3.3 Trivy: 8
2.3.4 Snyk: Monitoraggio Continuo 8

Capitolo 1

Introduzione

In un'epoca in cui il software permea ogni aspetto della vita quotidiana, la sicurezza informatica è diventata una pietra angolare nello sviluppo e nel deployment delle applicazioni. La continua espansione dell'utilizzo dei container e delle microservizi ha portato alla necessità di strumenti sofisticati capaci di identificare e mitigare le vulnerabilità in modo efficace ed efficiente. Questo report si propone di esplorare e confrontare due dei più rilevanti strumenti nel panorama della sicurezza informatica: Trivy e Snyk. Entrambi gli strumenti hanno guadagnato notorietà per la loro capacità di fornire analisi dettagliate e soluzioni alle vulnerabilità di sicurezza in applicazioni e container, ma presentano approcci, caratteristiche e punti di forza distinti.

Trivy

Trivy, sviluppato da Aqua Security, è un scanner di vulnerabilità semplice e completo, che si distingue per la sua facilità d'uso e la capacità di integrarsi senza soluzione di continuità in vari ambienti di sviluppo e pipeline CI/CD. La sua progettazione si concentra sulla velocità e sull'efficacia della scansione di immagini di container, repository Git, filesystem e configurazioni Infrastructure as Code (IaC), rendendolo uno strumento versatile per gli sviluppatori e i team di sicurezza.

Snyk

Snyk si posiziona come una soluzione SaaS di sicurezza per lo sviluppo software che enfatizza la collaborazione tra sviluppatori e professionisti della sicurezza. Offre una vasta gamma di funzionalità che vanno oltre la semplice scansione delle vulnerabilità, inclusa la gestione delle dipendenze, la correzione automatica e l'integrazione profonda con ambienti di sviluppo, sistemi di gestione del codice sorgente e pipeline di CI/CD. Snyk mira a dotare i team di strumenti proattivi per affrontare le vulnerabilità all'interno del loro codice, delle dipendenze open source, dei container e delle configurazioni IaC.

1.1 Processo di scansione

1.1.1 Trivy

I tool effettuano il processo di scansione delle vulnerabilità in container Docker modi diversi:

Trivy utilizza il comando di scansione `trivy image` per eseguire la scansione di un'immagine Docker. Questo comando esegue automaticamente tre funzioni:

- **Download del database delle vulnerabilità**: Trivy scarica automaticamente l'ultima versione del database delle vulnerabilità dalla repository ufficiale.
- **Scansione dell'immagine**: Trivy esegue la scansione dell'immagine Docker specificata, identificando e classificando le vulnerabilità presenti nei pacchetti e nelle librerie. Nel processo di scansione, Trivy analizza i file presenti nell'immagine, identificando le versioni dei pacchetti e confrontandole con il database delle vulnerabilità. Nel processo, vengono scansionate quattro categorie di problemi:
  - **Vulnerabilità**: problemi di sicurezza noti e documentati, che possono essere sfruttati da attaccanti per compromettere l'integrità e la disponibilità del sistema.
  - **Configurazioni errate**: errori di configurazione e di implementazione che possono esporre il sistema a rischi di sicurezza.
  - **Segreti e chiavi di accesso**: presenza di segreti e chiavi di accesso non crittografate all'interno dell'immagine, che possono essere sfruttati da attaccanti per ottenere accesso non autorizzato al sistema.
  - **Licenze:** presenza di licenze non conformi o non autorizzate all'interno dell'immagine, che possono esporre il sistema a rischi legali e di sicurezza.

  Di default, Trivy esegue la scansione di tutte e quattro le categorie, ma è possibile specificare una categoria specifica da scansionare utilizzando l'opzione `-scanners <vuln_type>`.
- **Generazione del report**: Trivy genera un report dettagliato delle vulnerabilità rilevate, classificandole in base al loro grado di gravità e fornendo informazioni dettagliate sulle azioni consigliate per mitigarle. Il punteggio di gravità di una vulnerabilità è assegnato tramite il sistema CVSS (Common Vulnerability Scoring System).

1.1.2 Snyk

Snyk opera invece secondo un processo differente, approcciando la scansione delle vulnerabilità direttamente dai momenti di stesura del codice. Esso è infatti suddiviso in quattro componenti principali:

- **Snyk Code:** componente relativo all'analisi statica. In questo passaggio, viene analizzato il codice sorgente per identificare i possibili problemi di sicurezza presenti nel codice. È possibile integrare Snyk Code con ambienti di sviluppo (es. Visual Studio Code) o sistemi di gestione del codice sorgente (es. Git), per eseguire automaticamente la scansione del codice sorgente, ad esempio all'esecuzione di un nuovo commit. Gli eventuali problemi di sicurezza rilevati vengono notificati all'utente tramite l'interfaccia web di Snyk, con un'evidenziazione delle linee di codice interessate e delle azioni consigliate per mitigare i problemi, come riportato in figura 1.1.

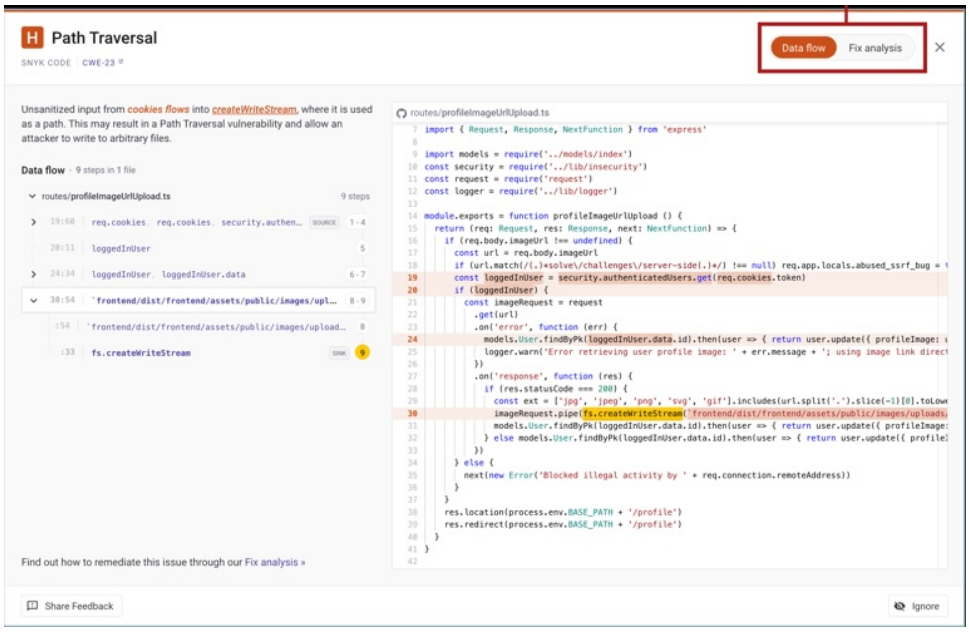

Figura 1.1: Risultato della scansione del codice sorgente con Snyk Code

- **Snyk Container:** il vero e proprio strumento per l'analisi delle vulnerabilità. Questo processo è suddiviso in tre fasi principali:
  - **Download dell'immagine**: l'immagine viene automaticamente scaricata in locale per permetterne l'analisi.
  - **Ottenimento della lista del software installato:** Snyk cerca il software installato all'interno dell'immagine. La ricerca viene effettuata in base a tre criteri:
    * Software installato tramite package manager (es. apt, yum, apk)
    * Software comunemente installato, e residente in posizioni predefinite
    * Applicazioni basate sulla presenza di un file manifest (es. package.json, requirements.txt)
  - **Invio delle vulnerabilità a Snyk:** La lista del software trovato viene inviata tramite API a Snyk, la quale confronta i dati con il suo database di vulnerabilità. Le vulnerabilità trovate vengono quindi restituite all'utente.
- **Snyk Open Source:** Snyk Open Source è uno strumento di analisi delle vulnerabilità per le dipendenze open source, che identifica e classifica le vulnerabilità presenti nelle librerie e nei pacchetti utilizzati all'interno del codice sorgente. Snyk Open Source è in grado di eseguire la scansione delle dipendenze open source, identificando le vulnerabilità e fornendo informazioni dettagliate sulle azioni consigliate per mitigarle.
- **Snyk Infrastructure as Code (IaC):** Snyk IaC è uno strumento di analisi delle vulnerabilità per le configurazioni Infrastructure as Code (IaC), che identifica e classifica le vulnerabilità presenti nei file di configurazione di Terraform, CloudFormation e altri strumenti di automazione dell'infrastruttura. Snyk IaC è in grado di eseguire la scansione delle configurazioni IaC, identificando le vulnerabilità e fornendo informazioni dettagliate sulle azioni consigliate per mitigarle.

Capitolo 2

Confronto

2.1 Scansione delle vulnerabilità

Il database di entrambi gli strumenti è un aspetto cruciale per la qualità e l'accuratezza delle analisi di vulnerabilità. Trivy e Snyk utilizzano database di vulnerabilità differenti, che influenzano la loro capacità di identificare e classificare le vulnerabilità.
In questa parte di testing, si è voluto valutare la capacità di Trivy e Snyk di identificare e classificare le vulnerabilità in base al database utilizzato. Per fare ciò, si è utilizzato un campione di immagini di container e repository Git, contenenti vulnerabilità note e ben documentate, e si è confrontato il risultato delle scansioni di Trivy e Snyk con le informazioni disponibili nei database VulnDB e Snyk. I risultati di questo test sono stati valutati in base alla precisione, alla completezza e alla tempestività delle informazioni fornite da Trivy e Snyk, e alla loro capacità di identificare e classificare le vulnerabilità in base al database utilizzato. L'aggiornamento dei database avviene per ogni tool in modo differente. Trivy, infatti, controlla la presenza di aggiornamenti del database ad ogni esecuzione, e scarica automaticamente la versione più recente. Snyk, invece, offre la possibilità di aggiornare manualmente il database, ma non è possibile controllare la presenza di aggiornamenti in modo automatico.
Le immagini Docker sottoposte a scansione sono state selezionate in base alla loro popolarità e alla loro rilevanza nel panorama delle applicazioni e dei servizi cloud. In particolare, si è scelto di testare le seguenti immagini:

- **nginx**: uno dei più popolari server web e reverse proxy.
- **mongo**: database NoSQL flessibile e scalabile basato su MongoDB.
- **wordpress**: piattaforma di blogging e CMS basata.
- **alpine**: una delle immagini di container più leggere e minimali, basata su Alpine Linux, che offre un ambiente di esecuzione ideale per applicazioni e servizi cloud.
- **centos**: una delle immagini di container più stabili e affidabili, basata su CentOS, che offre un ambiente di esecuzione robusto e ben supportato per applicazioni e servizi cloud.

In particolare, si è voluto testare due tipi di versioni: la versione più recente, e una versione più datata. Nella tabella **??** sono riportati i risultati ottenuti da entrambi i tool per ciascuna immagine testata.

Immagine	Vers.	Snyk				Trivy			
		Crit.	High	Mid	Low	Crit.	High	Mid	Low
nginx	latest	0	1	2	3	2	16	34	83
	v1.23.0	10	39	73	111	16	80	139	115
mongo	latest	0	0	0	0	0	0	1	21
	v4.4.3	0	0	0	0	0	0	0	0
wordpress	latest	0	0	0	0	0	0	0	0
	v6.0.0	0	0	0	0	0	0	0	0
alpine	latest	0	0	0	0	0	0	0	0
	v3.11	0	0	0	0	0	0	0	0
node	latest	0	0	0	0	0	0	0	0
	v16.0.0	0	0	0	0	0	0	0	0

Tabella 2.1: Confronto tra strumenti per la sicurezza delle immagini Docker

2.2 Scansione di configurazioni IaC

Un'altra funzionalità offerta da entrambi i tool è relativa alla scansione di configurazioni IaC, al fine di rilevare problemi di sicurezza o cattive pratiche di configurazione. Per testare tale funzionalità, si è utilizzato un campione di file di configurazione di Terraform, appropriatamente configurato con una vulnerabilità di esempio nota e ben documentata. Questa vulnerabilità è rappresentata dalla configurazione errata delle politiche di accesso su un bucket S3 di AWS, il quale è stato impostato per permettere l'accesso in lettura al pubblico di tutto il bucket (public-read). Tale configurazione espone i dati contenuti nel bucket a potenziali accessi non autorizzati, rappresentando un rischio significativo per la sicurezza dei dati. Eseguendo la scansione del file con entrambi gli strumenti, sono state rilevate le seguenti vulnerabilità:

Strumento	Critical	High	Medium	Low
Snyk	0	0	1	3
Trivy	0	7	1	2

Come è possibile rilevare dal grafico, la scansione con Trivy ha rilevato un numero maggiore di vulnerabilità rispetto a Snyk, in particolare un numero maggiore di vulnerabilità di livello alto. Entrambi i tool sono stati in grado di identificare correttamente la vulnerabilità desiderata, nonostante il grado di gravità assegnato sia risultato differente.

2.3 Differenze di funzionalità

Durante il testing, sono state rilevate le seguenti funzionalità uniche per ciascuno strumento:

2.3.1 Trivy: scansione di cluster Kubernetes

Trivy offre la possibilità di eseguire la scansione di un intero cluster Kubernetes, identificando e classificando le vulnerabilità presenti nei pod, nei deployment e nei servizi. Questa funzionalità è particolarmente utile per i team di sicurezza e per gli amministratori di sistema, che possono utilizzare Trivy per identificare e mitigare le vulnerabilità in modo proattivo, prima che possano essere sfruttate da attaccanti. Durante il testing, si è verificato che Trivy è in grado di eseguire la scansione di un cluster Kubernetes in modo rapido ed efficiente, fornendo un report dettagliato delle vulnerabilità rilevate e delle azioni consigliate per mitigarle.

2.3.2 Trivy: Scansione delle Configurazioni Infrastructure as Code (IaC)

Trivy offre la possibilità di eseguire la scansione delle configurazioni Infrastructure as Code (IaC), identificando e classificando le vulnerabilità presenti nei file di configurazione di Terraform, CloudFormation e altri strumenti di automazione dell'infrastruttura. Questa funzionalità è particolarmente utile per i team di sviluppo e per gli amministratori di sistema, che possono utilizzare Trivy per identificare e mitigare le vulnerabilità nelle configurazioni IaC, prima che possano essere sfruttate da attaccanti. Durante il testing, si è verificato che Trivy è in grado di eseguire la scansione delle configurazioni IaC in modo rapido ed efficiente, fornendo un report dettagliato delle vulnerabilità rilevate e delle azioni consigliate per mitigarle.
Per testare tale funzionalità, si è utilizzato un campione di file di configurazione di Terraform, appropriamente configurato con una vulnerabilità di esempio nota e ben documentata. Questa vulnerabilità è rappresentata dalla configurazione errata delle politiche di accesso su un bucket S3 di AWS, il quale è stato impostato per permettere l'accesso in lettura al pubblico (public-read). Tale configurazione espone i dati contenuti nel bucket a potenziali accessi non autorizzati, rappresentando un rischio significativo per la sicurezza dei dati. Come è possibile osservare dalla figura 2.1, Trivy è stato in grado di identificare e classificare correttamente la vulnerabilità presente nella configurazione di Terraform, fornendo un report dettagliato delle azioni consigliate per mitigarla.

Figura 2.1: Risultato della scansione delle configurazioni IaC con Trivy

2.3.3 Trivy:

2.3.4 Snyk: Monitoraggio Continuo

Snyk offre un monitoraggio continuo delle applicazioni e delle dipendenze, inviando notifiche in tempo reale in caso di nuove vulnerabilità che influenzano il codice già in uso. Questo assicura che i team possano reagire rapidamente a nuove minacce. Durante il testing, è stato possibile osservare il funzionamento di questa funzione, avendo ricevuto e-mail contenenti nuove vulnerabilità pubblicate solamente giorni prima, come riportato in figura 2.2.

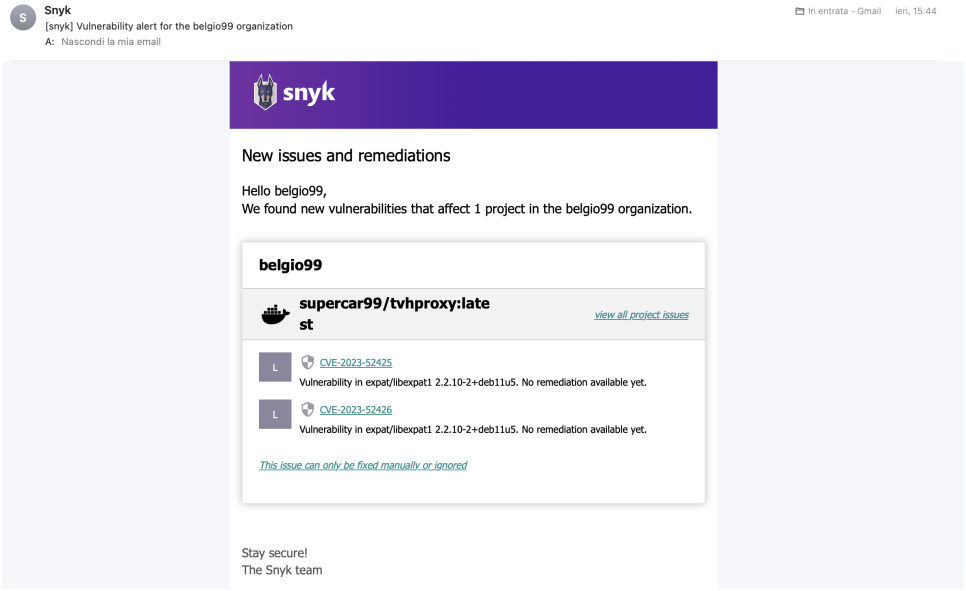

Figura 2.2: E-mail ricevuta da Snyk contenente notifica di rilevazione di nuove vulnerabilità

Dopo la ricezione della e-mail, è stata subito eseguita una scansione con Trivy, che ha confermato la presenza delle vulnerabilità segnalate da Snyk. Questo conferma che entrambi i database utilizzati da Trivy e Snyk sono aggiornati tempestivamente.