Relazione sull'Attività Svolta: Configurazione di Splunk su Windows 10 con VirtualBox

Introduzione

L'attività svolta si è concentrata sulla configurazione di due macchine virtuali Windows 10 N su VirtualBox, collegate in modalità bridge, e sull'installazione di **Splunk** e **Splunk Universal Forwarder** per monitorare e analizzare le attività di sistema. Splunk è uno strumento di monitoraggio che consente di raccogliere, indicizzare e visualizzare dati di log e metriche in tempo reale. Questa configurazione è utile per ottenere visibilità su eventi di sicurezza e performance di sistema.

Strumenti Utilizzati

- **VirtualBox**: software di virtualizzazione utilizzato per configurare due macchine virtuali.
- **Windows 10 N**: sistema operativo utilizzato sia per la macchina server sia per il client.
- **Splunk Enterprise**: installato sulla macchina Windows 10 N server per raccogliere e analizzare dati.
- **Splunk Universal Forwarder**: installato sulla macchina Windows 10 N client per inviare dati di log al server Splunk.
- **Modalità Bridge**: configurazione di rete che consente a ciascuna macchina virtuale di ottenere un IP direttamente dalla rete locale, simulando una vera connessione di rete.

Procedura

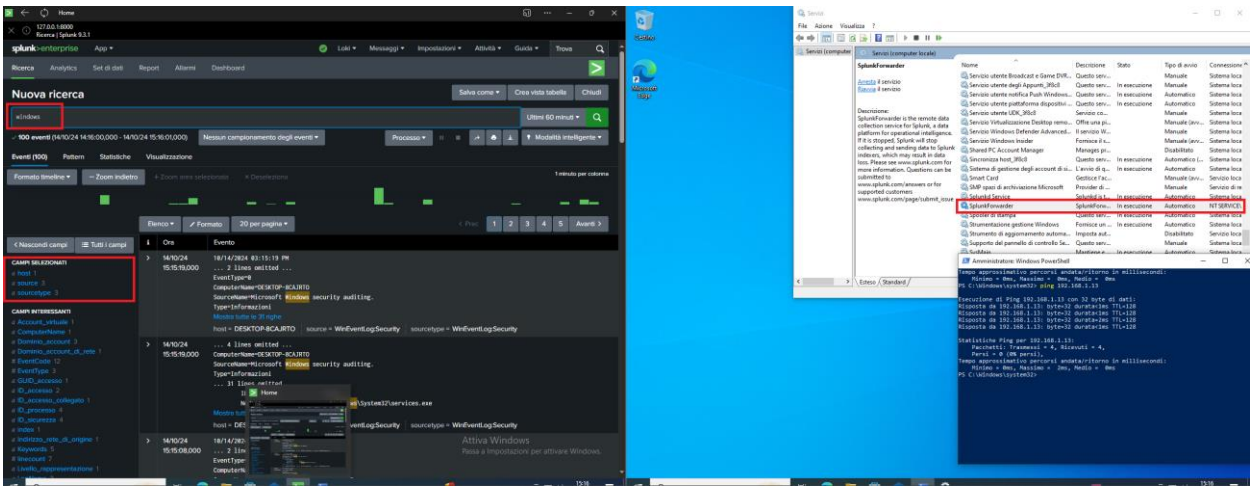
1. **Configurazione delle Macchine Virtuali su VirtualBox**:
    - Sono state create due macchine virtuali Windows 10 N su VirtualBox.
    - Le macchine sono state configurate in modalità **Bridge**, consentendo a ciascuna macchina di ottenere un indirizzo IP dalla rete locale. In questo modo, le due macchine potevano comunicare direttamente come se fossero fisicamente collegate alla stessa rete.
2. **Installazione di Splunk Enterprise (Server)**:
    - Splunk Enterprise è stato installato su una delle macchine Windows 10 N, che è stata configurata come **server Splunk**.
    - Al termine dell'installazione, Splunk è stato avviato e accessibile tramite un'interfaccia web utilizzando l'indirizzo IP della macchina server.
    - Configurazione dell'indice di raccolta dati e delle porte di comunicazione necessarie per ricevere i dati inviati dal client.
3. **Installazione di Splunk Universal Forwarder (Client)**:
    - Splunk Universal Forwarder è stato installato sull'altra macchina virtuale Windows 10 N (il client).
    - Il Forwarder è stato configurato per inviare i dati di log di sistema alla macchina server tramite il protocollo di rete.
    - Durante l'installazione, sono stati specificati l'indirizzo IP del server Splunk e la porta di comunicazione utilizzata per la trasmissione dei dati.
4. **Configurazione e Connessione del Forwarder**:
    - Dopo aver installato Splunk Universal Forwarder sul client, è stata configurata la macchina per inviare eventi di log e attività di sistema al server Splunk.
    - Sul server Splunk, sono stati configurati i percorsi dei dati da monitorare e si è verificato che i log provenienti dal client fossero ricevuti correttamente.

5. **Raccolta e Analisi dei Dati**:
    - Attraverso l'interfaccia web di Splunk, sono stati avviati i processi di ricerca e analisi dei dati provenienti dalla macchina client.
    - Sono stati visualizzati vari eventi e attività generiche del sistema operativo Windows, come la creazione, la modifica e l'accesso a file, processi in esecuzione e attività di sistema, inclusi i file di log del sistema operativo.

Risultati

La configurazione è stata completata con successo e il server Splunk ha ricevuto correttamente i dati di log inviati dal client tramite Universal Forwarder. Grazie agli strumenti di ricerca di Splunk, è stato possibile:

- Visualizzare **eventi di sistema** e **log di sicurezza**.
- Monitorare attività specifiche, come i tentativi di accesso al sistema, i cambiamenti ai file, e l'esecuzione di processi.
- Analizzare i **file di log** generati dal sistema operativo Windows, con la possibilità di filtrare e cercare eventi specifici.



Conclusioni

L'attività ha dimostrato come Splunk possa essere utilizzato efficacemente per raccogliere, monitorare e analizzare eventi di sistema e file di log provenienti da più macchine in rete. La configurazione di Splunk Universal Forwarder su un client Windows ha permesso di centralizzare la raccolta dei log, migliorando la visibilità sulle attività di sistema. Questa configurazione è particolarmente utile in contesti aziendali o in ambienti di laboratorio per il monitoraggio della sicurezza e delle prestazioni del sistema.