# Esercitazione S10/L1

In questa esercitazione ho utilizzato Splunk, un SIEM, configurandolo in modo da mostrare gli eventi sull'host collegato

## Dispositivi / Software utilizzati:

- Windows 10
- Windows Server 2022
- Splunk

## SIEM

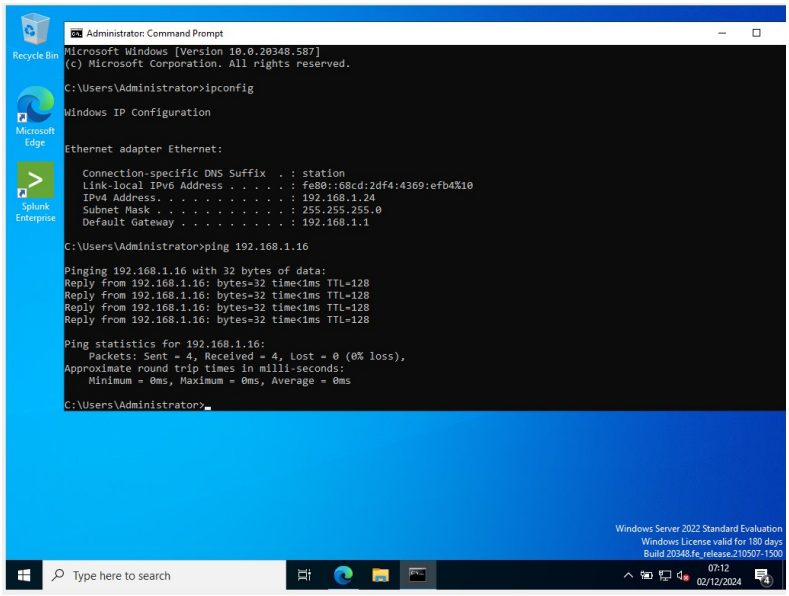
Un **SIEM** (Security Information and Event Management) è un sistema che raccoglie, analizza e gestisce i dati relativi alla sicurezza informatica di un'organizzazione. Questi dati includono log, eventi e avvisi provenienti da varie fonti, come firewall, endpoint, server, applicazioni e dispositivi di rete. Si tratta di uno strumento fondamentale in un **SOC** in quanto offre una visibilità centralizzata degli eventi e genera avvisi se ci sono dati anomali. Tutto ciò porta ad un monitoraggio e una risposta agli incidenti rapida ed efficace.

## Procedimento

Come prima cosa ho configurato le due macchine in modo che comunichino.

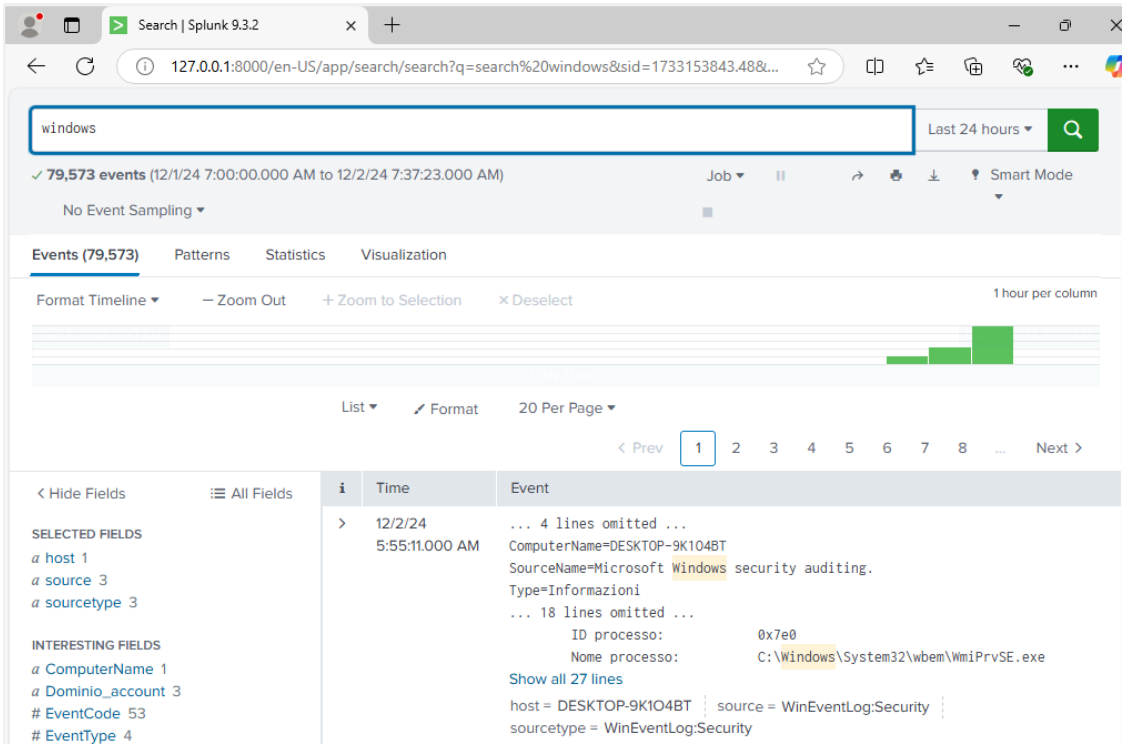
Ho poi proceduto con l'installazione di Splunk, il SIEM che andrò ad utilizzare per questa esercitazione.

Si procede con l'installazione di una parte Enterprise sulla macchina server (Windows Server 2022) e una parte Forwarder sulla parte Host (Windows 10), l'endpoint di riferimento.

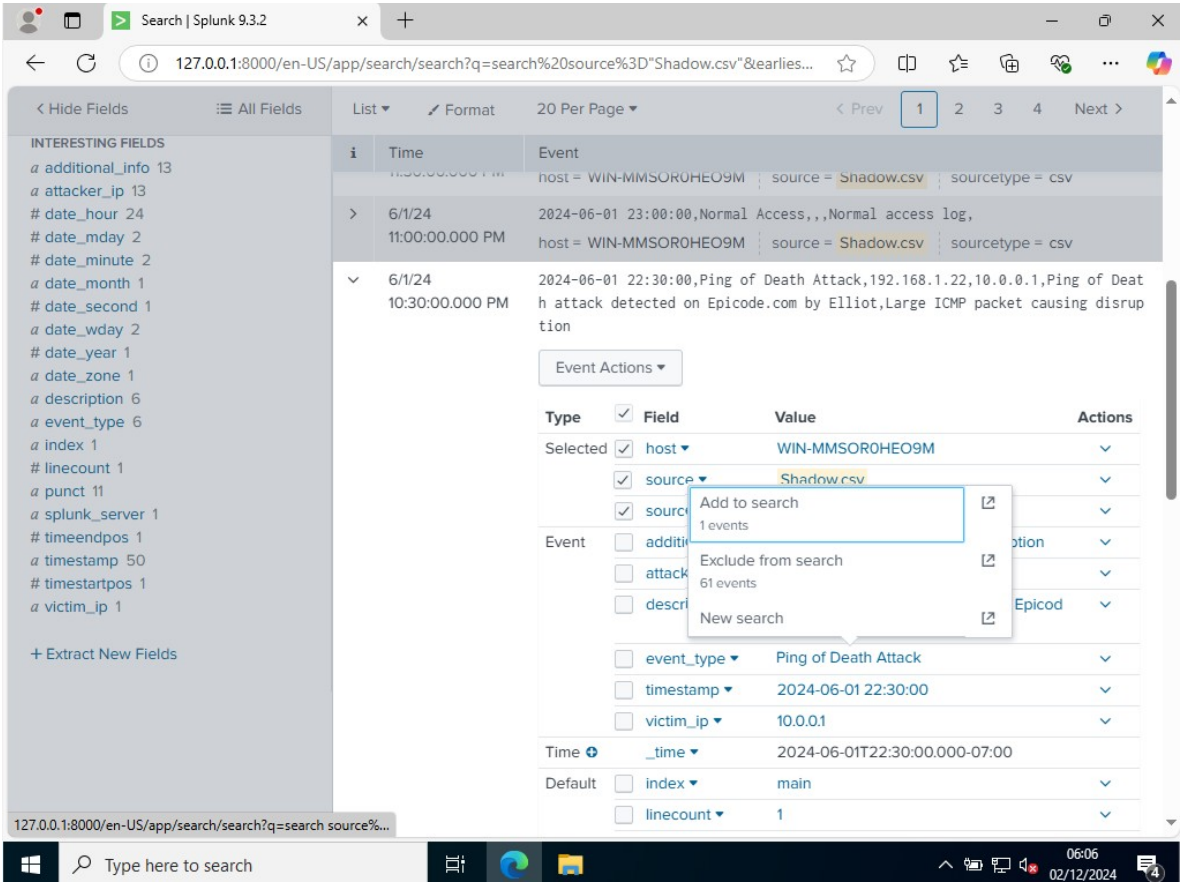



Impostate le porte di riferimento ho verificato, andando sulla modalità di monitoraggio di Splunk, se le macchine fossero in comunicazione.

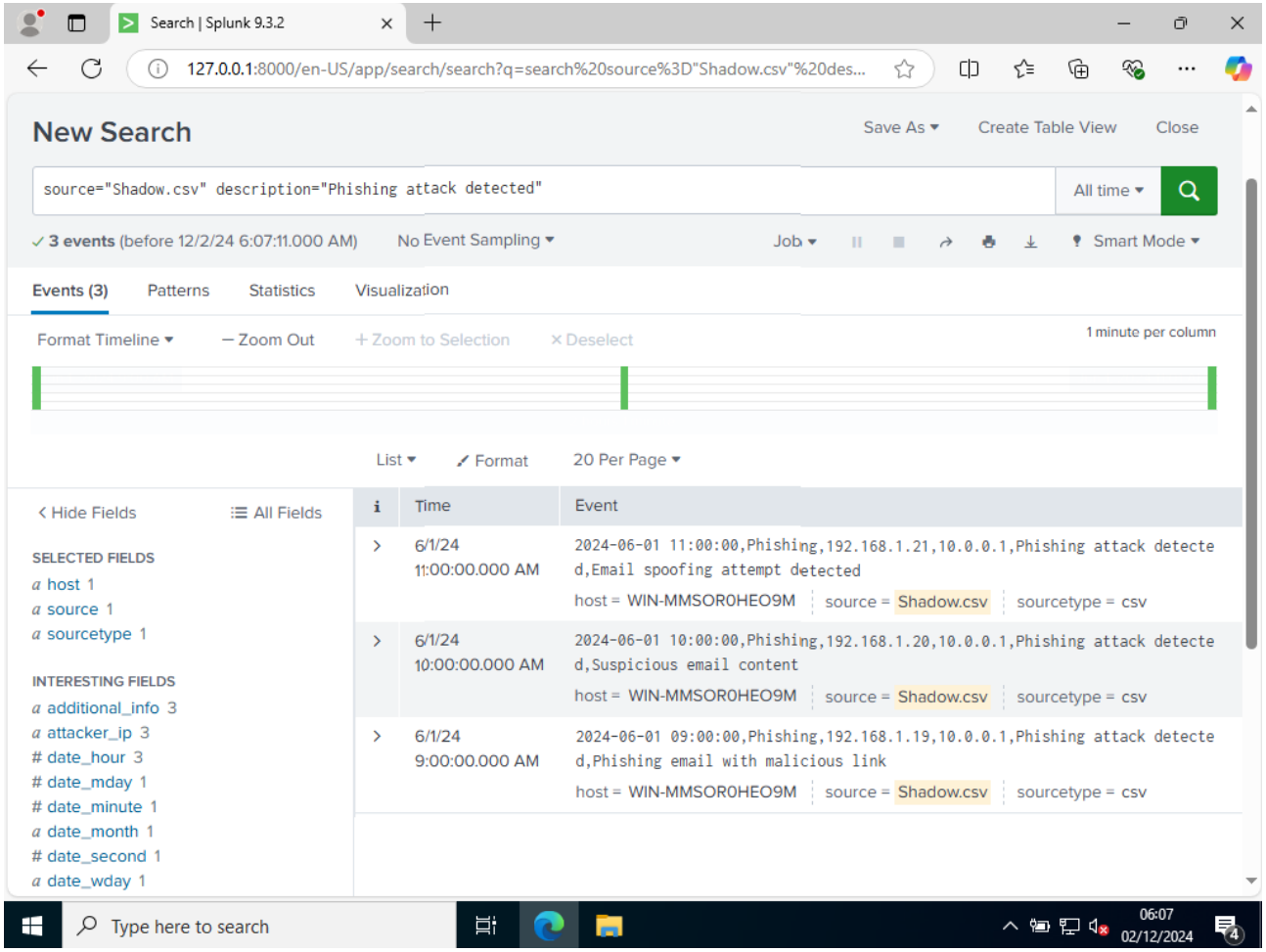
Si può notare nella foto la configurazione di Windows 10.




In questo modo posso confermare che la macchina Host è in comunicazione sulla macchina Server. Da questa schermata si possono vedere log, eventi e avvisi provenienti dall'Host.
Si possono ovviamente modificare le ricerche rendendole più specifiche per mostrare solo i risultati più attinenti alla ricerca, si può vedere infatti che sono stati trovati 79.573 eventi legati alla ricerca "windows".
Ho analizzato poi un altro file per vedere una simulazione più adeguata ad un ambiente di lavoro.



Si può vedere infatti l'esempio di un'evidenza di un attacco **Ping of death** tra gli eventi sull'Host in collegamento. Si possono anche vedere relativi dati o selezionare quel tipo di attacco per aggiungerlo nei filtri di ricerca.




Ho effettuato questa procedura con un altro tipo di attacco, **Phishing** in questo caso, che mi ha infatti evidenziato solo le tipologie di attacco phishing nella lista degli eventi. Dai 62 trovati senza filtri ne sono risultati solamente 3. Questa procedura è ottima per andare a visualizzare solo ciò che ci interessa in quel determinato momento.