Esercizio S10 L1 del 02/12/24 ***Daniele Paolone***

Siem Splunk

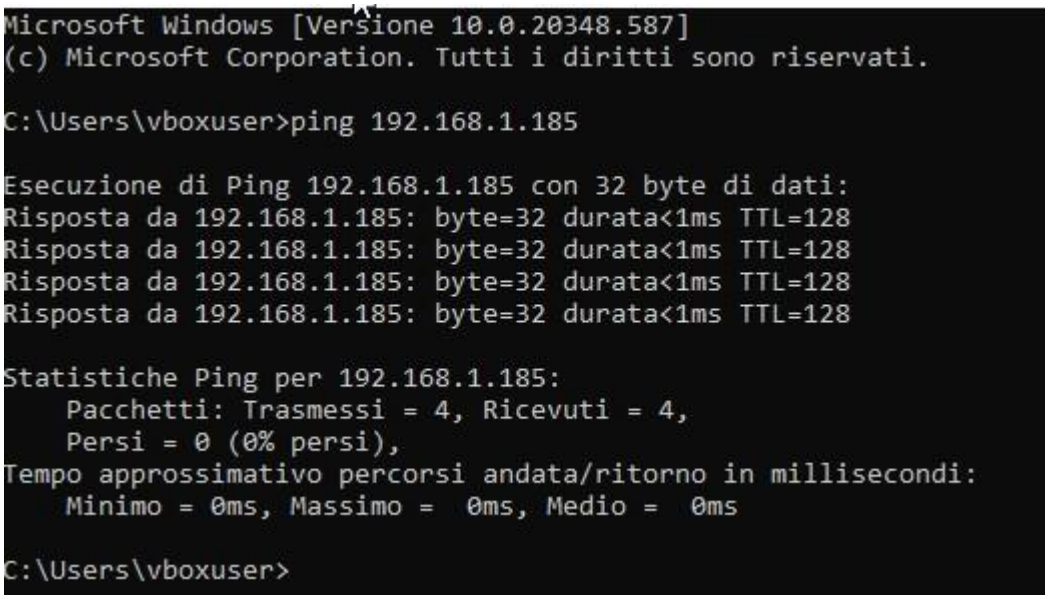
Un SIEM (*Security Information and Event Management*) è una piattaforma software che aiuta le organizzazioni a monitorare, analizzare e gestire la sicurezza delle loro reti e sistemi IT. Il SIEM raccoglie dati di log e eventi da varie fonti all'interno dell'infrastruttura IT, li analizza in tempo reale o in modo retrospettivo, e genera avvisi su attività sospette o potenziali minacce.

In particolare, si vedrà l'applicativo Splunk. Nell' esercizio si richiede di configurare la modalità Monitora e realizzare degli screenshot che mostrino l'esecuzione.

Prima fase

Si avviano le macchine virtuali di Windows Server e Windows 10 Pro. Successivamente si disattiva il firewall a Windows server, altrimenti non può avvenire il ping, che serve a verificare che le due macchine comunichino.

Ping effettuato da Windows Server con ip *192.168.1.158* a Windows 10 Pro con ip *192.168.1.185*.



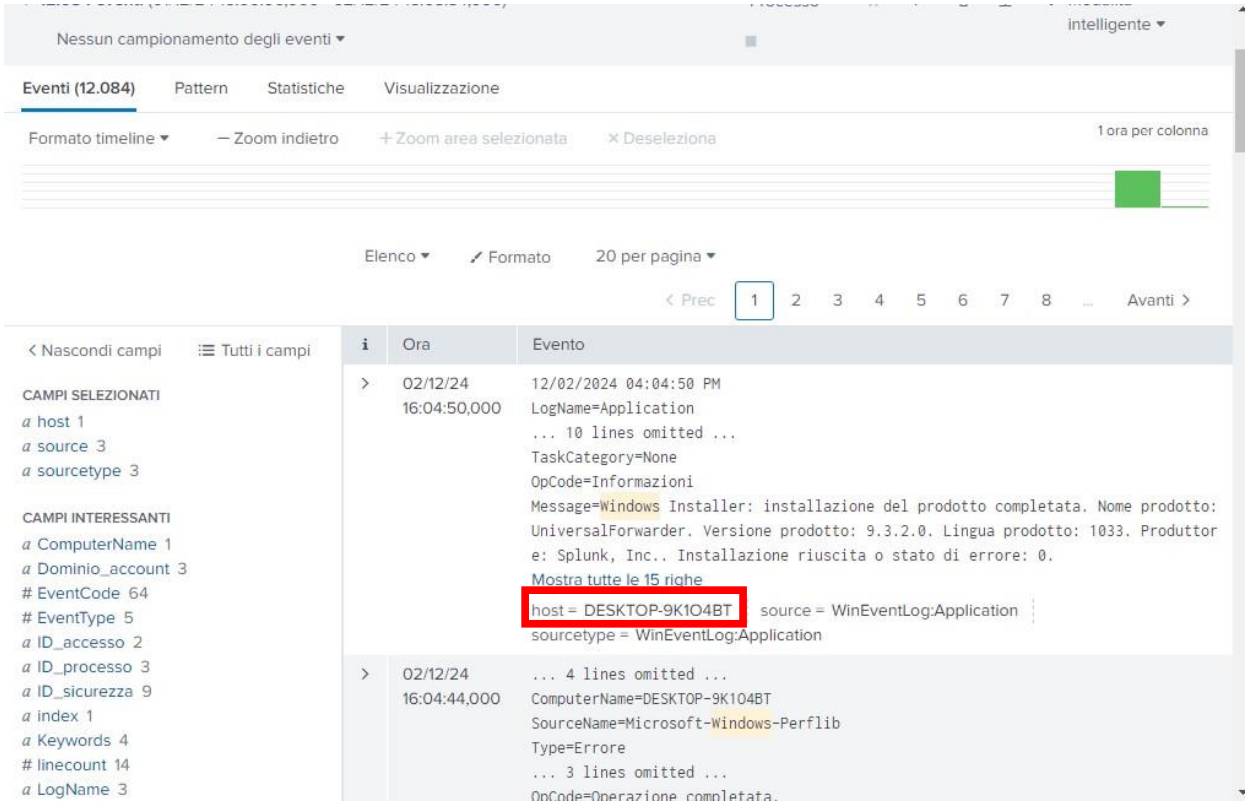
Ping effettuato da Windows 10 Pro con ip *192.168.1.185* a Windows Server con ip *192.168.1.158*.

Come si può notare dalle immagini, le macchine comunicano ed ora si può procedere alla seconda fase.

Seconda fase

Si installano i software Splunk Enterprise e SPlunk Forwarder, rispettivamente su Windows Server e Windows 10 Pro. Il primo serve a monitorare cosa avviene nel secondo, come in un vero ambiente aziendale.

Installato il tutto si avvia Splunk Enterprise e si accede alla sezione “cerca i tuoi dati”. Nella barra di ricerca di questa sezione si inserisce la parola “windows”. Il programma rilascerà una serie di eventi contenente questa parola.



Come si nota nell' immagine, nel primo evento della ricerca, compare il nome della macchina virtuale Windows 10 Pro e questo sta a significare che Splunk Enterprise riesce a monitorare ciò che avviene sull' altra macchina. Di seguito, come ulteriore prova, lo screenshot del nome della macchina preso dalle impostazioni di Sistema di Windows 10 Pro.