

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*.

```
Microsoft Windows [Versione 10.0.20348.587]
(c) Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\vboxuser>ping 192.168.1.185

Esecuzione di Ping 192.168.1.185 con 32 byte di dati:
Risposta da 192.168.1.185: byte=32 durata<1ms TTL=128
Risposta da 192.168.1.185: byte=32 durata<1ms TTL=128
Risposta da 192.168.1.185: byte=32 durata<1ms TTL=128
Risposta da 192.168.1.185: byte=32 durata<1ms TTL=128

Statistiche Ping per 192.168.1.185:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 0ms, Massimo = 0ms, Medio = 0ms

C:\Users\vboxuser>
```

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

```
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\user>ping 192.168.1.158

Esecuzione di Ping 192.168.1.158 con 32 byte di dati:
Risposta da 192.168.1.158: byte=32 durata<1ms TTL=128
Risposta da 192.168.1.158: byte=32 durata<1ms TTL=128
Risposta da 192.168.1.158: byte=32 durata<1ms TTL=128
Risposta da 192.168.1.158: byte=32 durata<1ms TTL=128

Statistiche Ping per 192.168.1.158:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 0ms, Massimo = 0ms, Medio = 0ms

C:\Users\user>
```

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.

Nessun campionamento degli eventi ▼

Intelligente ▼

Eventi (12.084) Pattern Statistiche Visualizzazione

Formato timeline ▼ — Zoom indietro + Zoom area selezionata × Deselezione 1 ora per colonna

Elenco ▼ ✎ Formato 20 per pagina ▼

< Prec 1 2 3 4 5 6 7 8 ... Avanti >

< Nascondi campi Tutti i campi

CAMPI SELEZIONATI

- a host 1
- a source 3
- a sourcetype 3

CAMPI INTERESSANTI

- a ComputerName 1
- a Dominio_account 3
- # EventCode 64
- # EventType 5
- a ID_accesso 2
- a ID_processo 3
- a ID_sicurezza 9
- a index 1
- a Keywords 4
- # linecount 14
- a LogName 3

i	Ora	Evento
>	02/12/24 16:04:50,000	12/02/2024 04:04:50 PM LogName=Application ... 10 lines omitted ... TaskCategory=None OpCode=Informazioni Message=Windows Installer: installazione del prodotto completata. Nome prodotto: UniversalForwarder. Versione prodotto: 9.3.2.0. Lingua prodotto: 1033. Produttore: Splunk, Inc.. Installazione riuscita o stato di errore: 0. Mostra tutte le 15 righe host = DESKTOP-9K1O4BT source = WinEventLog:Application sourcetype = WinEventLog:Application
>	02/12/24 16:04:44,000	... 4 lines omitted ... ComputerName=DESKTOP-9K1O4BT SourceName=Microsoft-Windows-Perflib Type=Errore ... 3 lines omitted ... OpCode=Operazione completata.

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.

Visualizza informazioni di base relative al computer

Edizione Windows

Windows 10 Pro

© 2015 Microsoft Corporation. Tutti i diritti sono riservati.

[Avanti](#)



Sistema

Processore: AMD Ryzen 5 5600G with Radeon Graphics 3.90 GHz
Memoria installata (RAM): 2,00 GB
Tipo sistema: Sistema operativo a 64 bit, processore basato su x64
Penna e tocco: Nessun input penna o tocco disponibile per questo schermo

Impostazioni relative a nome computer, dominio e gruppo di lavoro

Nome computer: DESKTOP-9K1O4BT
Nome completo computer: DESKTOP-9K1O4BT
Descrizione computer:
Gruppo di lavoro: WORKGROUP

[Cambia impostazioni](#)

Attivazione di Windows

Connettersi a Internet per attivare Windows. [Leggere le Condizioni di licenza software Microsoft](#)

Numero di serie: 00331-20305-79611-AA686

[Attiva Windows](#)