

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

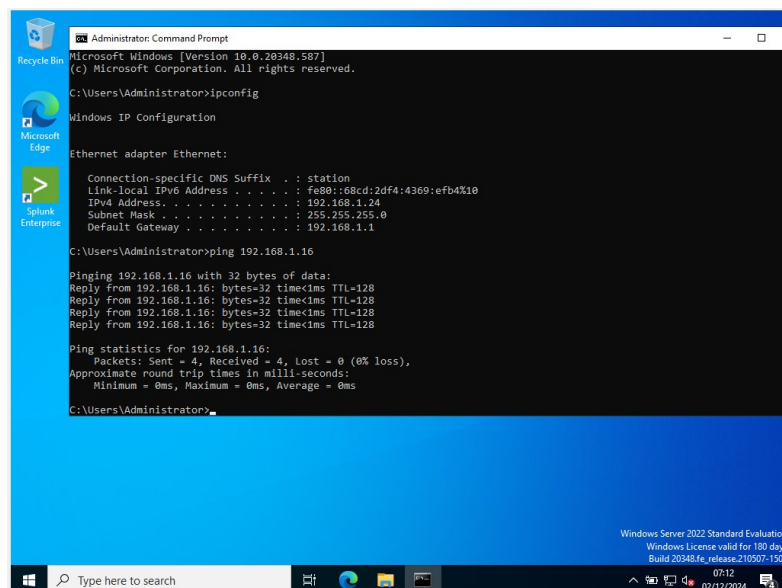
Un **SIEM** (Security Information and Event Management) è un sistema che raccoglie, analizza e gestisce i dati relativi alla sicurezza informatica di un'organizzazione. Questi dati includono log, eventi e avvisi provenienti da varie fonti, come firewall, endpoint, server, applicazioni e dispositivi di 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.

PC

Nome PC DESKTOP-9K1O4BT

Rinomina PC

Organizzazione WORKGROUP

Aggiungi a un dominio

Connetti ad Azure AD

Edizione Windows 10 Pro

ID prodotto 00331-20305-79611-AA686

Processore 12th Gen Intel(R) Core(TM) i7-1255U 2.61 GHz

RAM installata 2,00 GB

Tipo sistema Sistema operativo a 64 bit, processore basato su x64

The screenshot shows the Splunk Search interface with the search term "windows". The results show 79,573 events from 12/1/24 7:00:00.000 AM to 12/2/24 7:37:23.000 AM. The interface includes a search bar, a timeline visualization, and a list of events. The selected event is from 12/2/24 at 5:55:11.000 AM, with the event type "Windows security auditing". The event details show the computer name "DESKTOP-9K104BT", source name "Microsoft Windows", and type "Informazioni". The event ID is "0x7e0" and the process name is "C:\Windows\System32\wbem\WmiPrvSE.exe". The host is "DESKTOP-9K104BT" and the source is "WinEventLog:Security".

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.

The screenshot shows the Splunk Search interface with the search term "Shadow.csv". The results show 61 events from 2024-06-01 22:30:00.000 PM to 2024-06-01 22:30:00.000 PM. The interface includes a search bar, a timeline visualization, and a list of events. The selected event is from 2024-06-01 at 22:30:00.000 PM, with the event type "Ping of Death Attack". The event details show the host "WIN-MMSOR0HEO9M", source "Shadow.csv", and type "Ping of Death Attack". The event ID is "0x7e0" and the process name is "C:\Windows\System32\wbem\WmiPrvSE.exe". The host is "DESKTOP-9K104BT" and the source is "WinEventLog:Security".

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.

The screenshot shows the Splunk Search interface with the following details:

- Search Bar:** Contains the query `source="Shadow.csv" description="Phishing attack detected"` and a search button.
- Results Summary:** Shows 3 events found before 12/2/24 6:07:11.000 AM.
- Event List:** Displays three events with the following details:

i	Time	Event
>	6/1/24 11:00:00.000 AM	2024-06-01 11:00:00,Phishing,192.168.1.21,10.0.0.1,Phishing attack detected,Email spoofing attempt detected host = WIN-MMSOR0HEO9M source = Shadow.csv sourcetype = csv
>	6/1/24 10:00:00.000 AM	2024-06-01 10:00:00,Phishing,192.168.1.20,10.0.0.1,Phishing attack detected,Suspicious email content host = WIN-MMSOR0HEO9M source = Shadow.csv sourcetype = csv
>	6/1/24 9:00:00.000 AM	2024-06-01 09:00:00,Phishing,192.168.1.19,10.0.0.1,Phishing attack detected,Phishing email with malicious link host = WIN-MMSOR0HEO9M source = Shadow.csv sourcetype = csv
- Fields Panel:** On the left, it lists 'SELECTED FIELDS' (host, source, sourcetype) and 'INTERESTING FIELDS' (additional_info, attacker_ip, date_hour, date_mday, date_minute, date_month, date_second, date_wday).

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.