“Detection and Analysis of Web Authentications in a DMZ Environment”

Introduzione

Questo progetto nasce con l’obiettivo di simulare un’attività tipica di un Security Operations Center (SOC) di livello 1, focalizzata sulla rilevazione e analisi di attività potenzialmente malevole dirette verso un sistema esposto in rete.

In particolare, il laboratorio è progettato per dimostrare come un analista SOC possa:

- raccogliere e centralizzare log provenienti da ambienti eterogenei,
- individuare comportamenti anomali su servizi legittimamente esposti,
- distinguere attività malevole da traffico e accessi legittimi,
- effettuare un primo livello di triage basato su evidenze oggettive.

Il focus non è la prevenzione dell’attacco, ma la detection e l’analisi post-evento, in linea con le responsabilità operative di un SOC Level 1.

Contesto (SOC Level 1)

Nel contesto aziendale reale, i servizi esposti in **DMZ** rappresentano una delle superfici di attacco più comuni. Web server e servizi di accesso remoto, pur essendo necessari per motivi operativi, sono frequentemente bersaglio di:

- tentativi di accesso non autorizzato,
- brute force su credenziali,
- attività di scanning ed enumerazione.

In questo scenario, il traffico che raggiunge il sistema **non viola necessariamente le policy di rete**, ma può comunque indicare un comportamento ostile.
Per questo motivo, la rilevazione viene demandata a strumenti di **monitoraggio e analisi dei log**, come un SIEM, piuttosto che a controlli di perimetro.

Topologia di rete

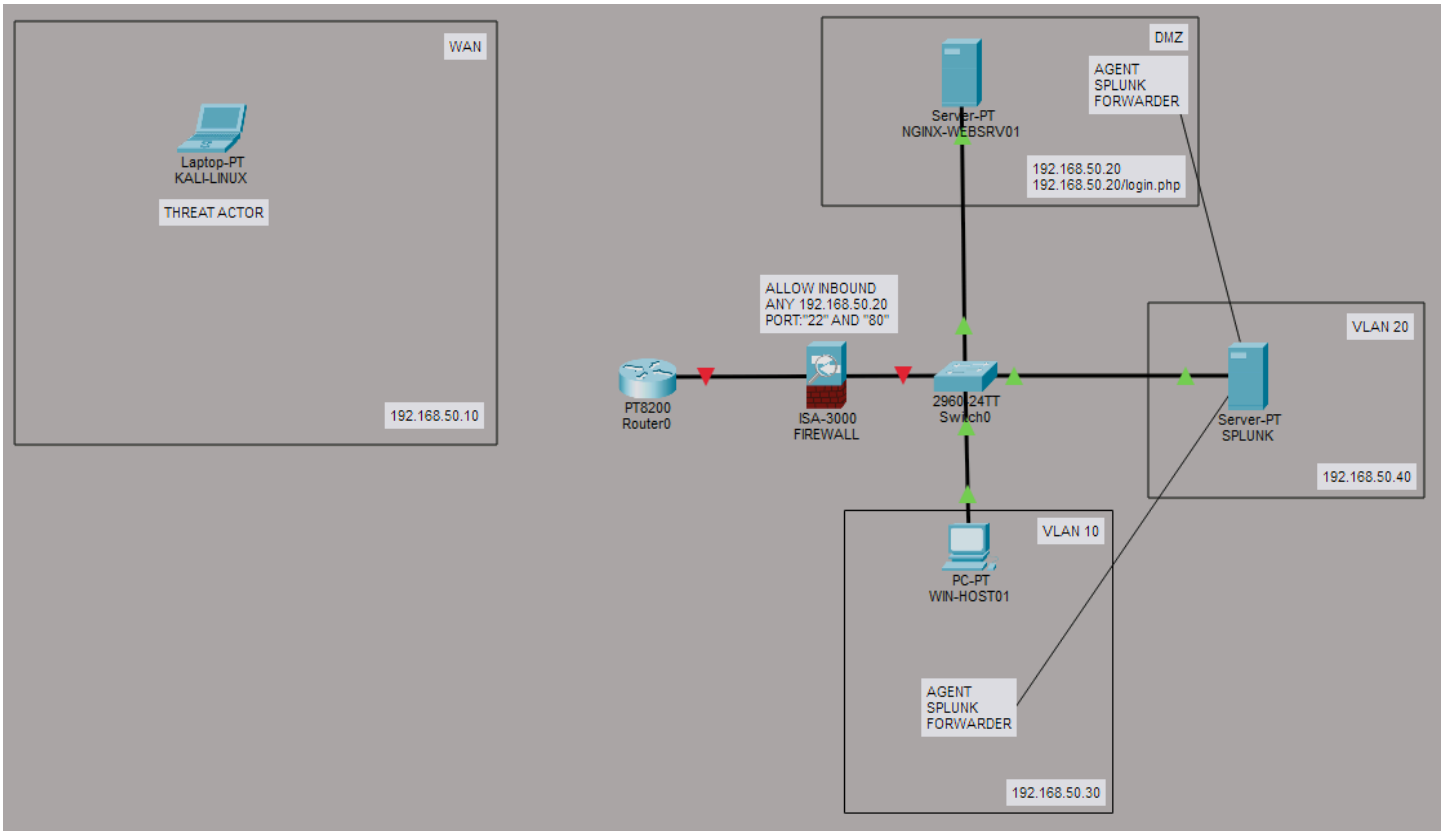
L’ambiente di laboratorio è strutturato per simulare una **architettura aziendale semplificata ma realistica**, composta da una rete perimetrale (DMZ), una rete interna e un sistema centralizzato di monitoraggio.

La topologia è progettata per riflettere un contesto in cui:

- alcuni servizi sono **volutamente esposti verso l’esterno**,
- altri sistemi operano esclusivamente in ambito interno,
- la sicurezza non è demandata a un singolo controllo, ma distribuita tra **perimetro, host e monitoraggio**.

L’architettura si articola nei seguenti domini di rete:

- **WAN / External Network**
- **DMZ**
- **Internal Network**
- **Monitoring Network (SIEM)**



Segmentazione di rete

WAN / External Network

Rappresenta l'ambiente esterno non fidato, da cui opera il **Threat Actor**.
Da questa rete originano i tentativi di accesso e le attività di scanning dirette verso i servizi pubblicamente esposti.

DMZ (Demilitarized Zone)

La DMZ ospita un **Web Server Linux**, configurato per fornire servizi legittimi:

- accesso remoto tramite **SSH**,
- servizio **HTTP** tramite web server (Nginx).

Il sistema in DMZ è intenzionalmente esposto:

- il traffico in ingresso è consentito dalle policy di rete,
- l'analisi del rischio avviene **a posteriori**, tramite log applicativi e di sistema.

Sul web server è installato lo **Splunk Universal Forwarder**, incaricato di raccogliere e inoltrare i log di autenticazione e di accesso web al SIEM centrale.

Internal Network

La rete interna ospita un **host Windows** che rappresenta un sistema legittimo utilizzato da utenti aziendali.
Questo sistema genera:

- eventi di autenticazione,
- attività di sistema normali,
- traffico applicativo legittimo.

I log prodotti dall'host Windows costituiscono una **baseline di comportamento normale**, utile per confrontare e distinguere l'attività malevola proveniente dalla DMZ.

Anche su questo sistema è presente uno **Splunk Universal Forwarder** per l'invio degli eventi al SIEM centralizzato.

Monitoring Network (SIEM)

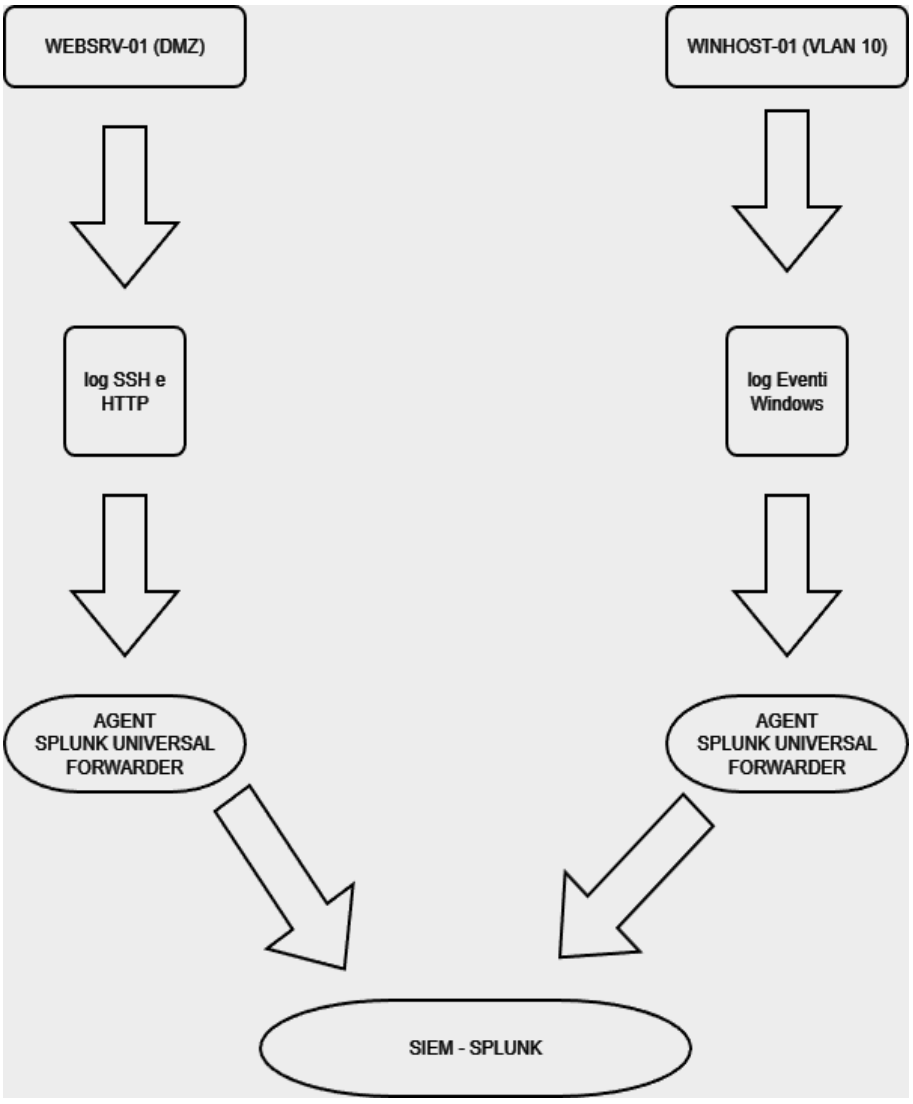
Il **Splunk Server** è collocato in una rete separata, con il solo ruolo di:

- ricevere i log dagli host monitorati,
- indicizzare gli eventi,
- consentire l'analisi e il triage da parte dell'analista SOC.

Il SIEM **non è direttamente esposto** verso la rete esterna e non partecipa al flusso applicativo, ma opera esclusivamente come componente di monitoraggio.

Ruolo del firewall perimetrale

Tra la rete esterna e la DMZ è posizionato un **firewall perimetrale**, configurato per applicare controlli di accesso basati su policy. Le regole implementate consentono il traffico in ingresso verso il web server in DMZ sulle porte **22 (SSH)** e **80 (HTTP)**.



Flusso dei log

Tutti i sistemi monitorati inoltrano i propri eventi al SIEM centrale secondo il seguente flusso:

- Web Server (DMZ) - log SSH e HTTP - Splunk Universal Forwarder - Splunk Server
- Host Windows (Internal) - log di sistema e autenticazione - Splunk Universal Forwarder - Splunk Server

Scenario di Attacco

Lo scenario simulato riproduce una situazione comune in ambienti aziendali reali, in cui un sistema collocato in **DMZ** espone servizi necessari al funzionamento operativo, ma inevitabilmente visibili dall'esterno. In questo contesto, l'attaccante non possiede informazioni preventive sull'infrastruttura interna e agisce in modo opportunistico, limitandosi a individuare e testare i servizi pubblicamente accessibili.

L'attività ostile inizia con una fase di **reconaissance**, durante la quale l'attaccante esegue una scansione di rete sul perimetro esposto. Attraverso questa fase vengono individuate due porte aperte sul web server in DMZ: **la porta 80 (HTTP)** e **la porta 22 (SSH)**. La presenza di questi servizi indica un sistema operativo raggiungibile, potenzialmente interessante come bersaglio.

L'intero scenario è costruito per evidenziare come, in assenza di meccanismi di prevenzione avanzata, l'individuazione dell'attività malevola avvenga **a posteriori**, attraverso l'analisi dei log. Il focus non è dimostrare una compromissione riuscita, ma osservare e distinguere comportamenti anomali da attività operative normali, ponendo le basi per una corretta attività di **detection e triage** da parte di un analista SOC.

Fonti di Log e Raccolta Dati

La rilevazione delle attività descritte nello scenario si basa esclusivamente sull'analisi dei log generati dai sistemi coinvolti. Non vengono utilizzati meccanismi di ispezione del traffico in tempo reale né strumenti di prevenzione inline. Tutta la visibilità è ottenuta **a posteriori**, attraverso eventi registrati a livello di sistema e applicazione. I log vengono raccolti localmente sugli host e inoltrati al SIEM centrale tramite **Splunk Universal Forwarder**, configurato per monitorare specifiche fonti ritenute rilevanti per i casi d'uso di detection del progetto.

WEBSRV-01 (DMZ)

Il web server collocato in DMZ rappresenta il principale punto di osservazione dell'attività ostile. Su questo sistema vengono raccolti due insiemi di log distinti, ciascuno con un ruolo specifico nell'analisi. I **log di autenticazione SSH**, presenti nel file `/var/log/auth.log`, consentono di osservare i tentativi di accesso al sistema operativo, e in particolare ci permettono di distinguere i tentativi di accesso legittimi dai malevoli.

Accanto a questi, i **log di accesso HTTP** del web server, contenuti in `/var/log/nginx/access.log`, forniscono visibilità sull'interazione con il servizio web esposto. Da questi log è possibile analizzare il volume e la frequenza delle richieste, le risorse richieste, i codici di risposta HTTP, gli User-Agent e molto altro. Queste due fonti, analizzate congiuntamente, permettono di correlare le diverse fasi dell'attività dell'attaccante e di ricostruirne il comportamento nel tempo.

WINHOST-01 (Internal Network)

L'host Windows interno ha il ruolo di generare traffico e log **legittimi**, utili come riferimento comparativo. Su questo sistema vengono raccolti eventi dal **Windows Security Event Log**, in particolare quelli relativi all'autenticazione degli utenti. Nel contesto del progetto, tali eventi non sono analizzati come IoC, ma come **baseline di comportamento normale**, necessaria per distinguere attività lecite da pattern sospetti osservati sul sistema in DMZ.

Raccolta e inoltro dei log

Su entrambi i sistemi monitorati è installato lo **Splunk Universal Forwarder**, configurato per:

- monitorare le fonti di log di interesse,
- inoltrare gli eventi al SIEM centrale tramite connessione TCP sulla porta 9997.

Il forwarder opera come componente di raccolta e trasporto, senza effettuare alcuna analisi o filtraggio logico sugli eventi. La selezione dei log rilevanti e la loro interpretazione avviene esclusivamente a livello di SIEM.