22 NOVEMBRE 2025

W20D4-SOC,SIEM,SOAR

REPORT FINE MODULO

Luca Tipaldi

REPORT DI FINE MODULO

Azioni preventive: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato?

Le azioni preventive per difendere da questo tipo di attacchi possono essere :

1. Query parametrizzate : permette di trattare gli input inseriti dall'utente come dati e non come query valutando i parametri inseriti come stringhe.

Esempio :

```
SELECT * FROM utenti WHERE username = 'admin' AND password = '' OR
'1'='1'
```

'1'='1' è sempre vero → l'attaccante potrebbe entrare senza conoscere la password.

2. Validazione lato server : attraverso apposite policy impedire all'utente di inserire input inattesi come caratteri o formati speciali.

3. Principio del minimo privilegio : l'utente che ha accesso al database in cui risiedono i dati specifici non deve essere utente root e debba avere solo autorizzazioni necessarie come quelli di inserimento, modifica e aggiornamento.

4. Evitare di mostrare messaggi di errore dettagliati

5. Escaping : È un modo per fare in modo che il testo inserito dagli utenti non venga interpretato come codice HTML o JavaScript, ma rimanga semplice testo.

```
<script>alert("hack")</script> -> &lt;script&gt;alert("hack")&lt;/
script&gt;
```

In questo modo il browser non lo esegue.

6. Cookie sicuri: utilizzare flag come :

`HttpOnly ->` non accessibili da JavaScript : il cookie non compare in `document.cookie`

`Secure ->` solo su HTTPS

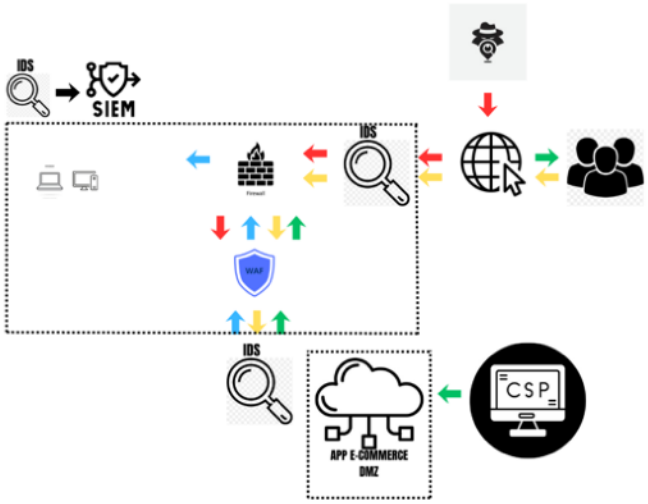
7. Content Security Policy (CSP)

Impostare l'header Content-Security-Policy per limitare da dove possono essere caricati script.

8. WAF

Mettere un Web Application Firewall (WAF) davanti all'app che riconosca pattern tipici di SQLi o XSS per bloccarli tempestivamente prima che arrivino al server

9. Aggiornamento patch, Backup e Cloud : azioni per recupero dei dati in caso di incidenti e prevenzioni delle eventuali falle nel sistema. Il cloud mette a disposizioni strumenti di sicurezza e di monitoraggio , rate limiting (per attacchi DDoS) e gestione dei permessi.



Blu -> Flusso applicazione ↔ rete interna

Rosso -> Traffico dell'attaccante verso l'e-commerce
Giallo -> Traffico utente verso l'e-commerce
Verde -> Applicazione e-commerce -> utente

Gli utenti si connettono da Internet all'applicazione e-commerce.
Prima di arrivare al cuore del sistema:

Controllo e sanificazione input

Un modulo filtra ciò che gli utenti inseriscono (parametri, form, cookie).
Protegge da: SQL Injection,Cross-Site Scripting e Manipolazioni varie dei parametri.

2. Zona Internet e primo livello di sicurezza

Subito dopo la connessione a internet, c'è:

IDS (Intrusion Detection System)

Un sistema che osserva il traffico e cerca comportamenti sospetti.
Se rileva un potenziale attacco, avvisa il SOC.

Non blocca direttamente, ma segnala.

3,4. Firewall / WAF nella DMZ

5.Il sistema e-commerce comunica anche con un ambiente cloud, ad esempio per: certificati,servizi esterni e autenticazione.

Anche questi passano attraverso IDS e WAF.

6. Rete interna aziendale

Qui lavorano gli operatori.
Accedono all'applicazione tramite un flusso blu, che passa attraverso firewall e viene monitorato.

La rete interna è isolata dall'esterno:
niente connessioni dirette utenti → rete interna
solo l'applicazione nella DMZ può parlare con la rete interna

7. SIEM/SOC (Security Operation Center)

Il cervello del sistema.

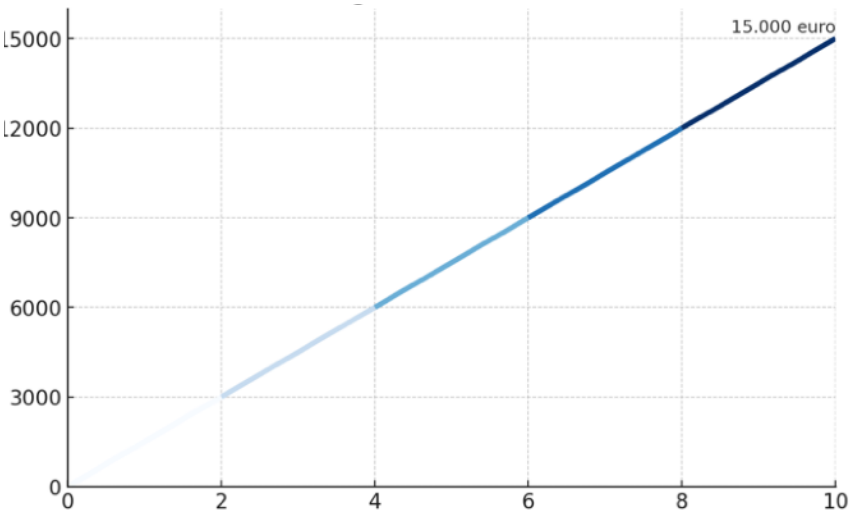
Riceve gli alert dagli IDS, fa: monitoraggio continuo,analisi degli incidenti,risposta agli attacchi e gestione delle vulnerabilità.

Impatti sul business: l'applicazione Web subisce un attacco di tipo DDoS dall'esterno che rende l'applicazione non raggiungibile per 10 minuti. Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce.

Per risolvere questo punto dell'esercizio basterà sostituire i dati della traccia alla seguente formula :

`CoD = ( GpM x TdI) + AC =`

1.500 x 10 = 15.000 euro



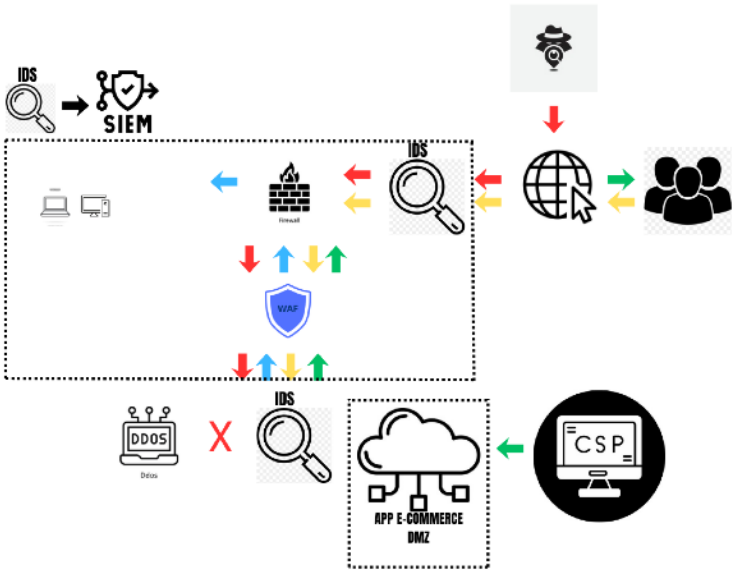
Le migliori soluzioni per prevenire un attacco DDoS sarebbero quelle di affidarsi ad un cloud, un server che offra importanti servizi per la sicurezza ma soprattutto avere più server distribuiti dove gestire ed indirizzare il traffico di rete (LOAD BALANCE) e lavorando insieme ad un WAF permettono di bloccare IP malevoli noti, richieste ripetitive con pattern tipici di not, pacchetti malformati.

La distribuzione del server permette dunque che la macchina target resti dunque isolata garantendo la Business Continuity.

Seppur vero che tale distribuzione permette una scalabilità orizzontale essa d'altro canto espone ad altre criticità come aumento della superficie d'attacco e cache poisoning.

Sarà opportuna affidarsi quindi a strumenti come IDS e IPS oltre che ad esempio ad un SIEM,uno strumento che raccoglie e analizza tutti i log dei sistemi per scoprire gli attacchi mentre accadono e aiutarti a rispondere velocemente e magari monitorare ad un certo intervallo di tempo lo stato della macchina (RAM e CPU).

Response: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta.

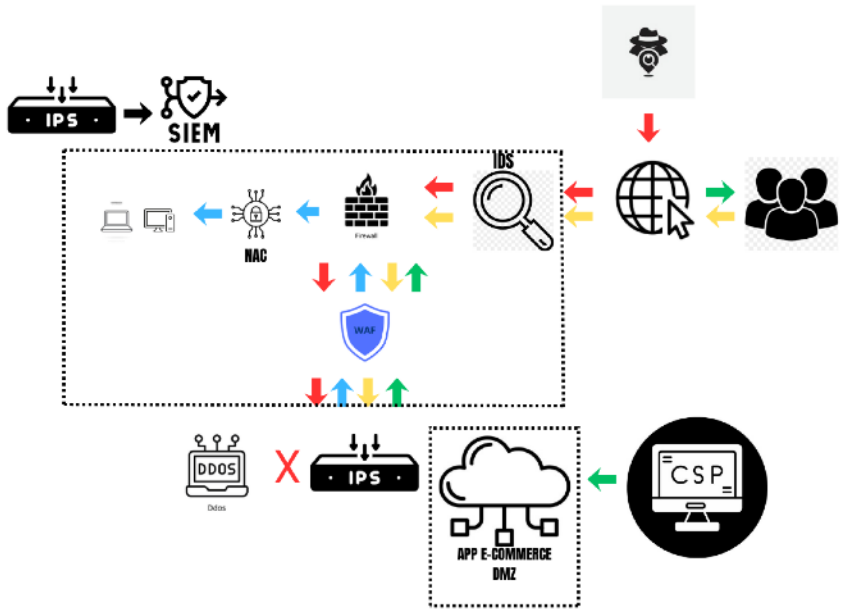


Lo schema rappresenta ciò che succede quando viene rilevato un attacco DDoS: il nostro sistema identifica la macchina compromessa e la isola automaticamente per proteggere l'intera infrastruttura.

La macchina infetta viene isolata per impedire che l'attacco si diffonda o saturi i servizi.

Il resto dell'infrastruttura rimane protetto e funzionante, perché il contenimento è immediato.
Questa è la fase di incident response: l'attacco è già in corso e la rete reagisce isolando la minaccia.

Soluzione completa: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3 e modifica «più aggressiva» dell'infrastruttura (se necessario/ facoltativo magari integrando la soluzione al punto 2).



Ho svolto i due punti dell'esercizio,integrando le due soluzione adottate in precedenza ed aggiungendo soluzioni di difesa più meticolose : NAC ed IPS.

Prima avevamo usato solo IDS che era necessaria alla detection, in questo caso abbiamo l'implementandola struttura di protezione in modo tale che essa blocchi attacchi in tempo reale, infatti può interrompere connessioni, scartare pacchetti o modificare percorsi e collaborare con firewall e NAC per isolare dispositivi. Inoltre è in grado di rilevare attacchi (come l'IDS),bloccare exploit e traffico malevolo,fermare brute force, DoS, malware ed applicare policy di prevenzione.

L'IPS non solo rileva, ma ferma.

L'IDS invece permette di identificare e isolare una macchina infetta per potervi accedere il futuro, studiare cosa sia successo e prevenire il riverificarsi dell'azione che hanno portato all'anomalia.

Un altro strumento di protezione avanzata è rappresentato dal NAC, il quale controlla chi e che cosa può collegarsi alla rete aziendale, oltre al come può farlo.

Non solo, il NAC controlla chi entra in rete,verifica la sicurezza dei dispositivi,applica regole di accesso basate sull'identità ed isola automaticamente minacce e dispositivi non conformi.

È un componente essenziale quando si vuol evitare che un dispositivo compromesso diventi un problema per tutta la rete.