Studente: Isabelle Adjetey
Corso Cybersecurity & Ethical Hacking

Progetto Fine Modulo 5

Traccia:

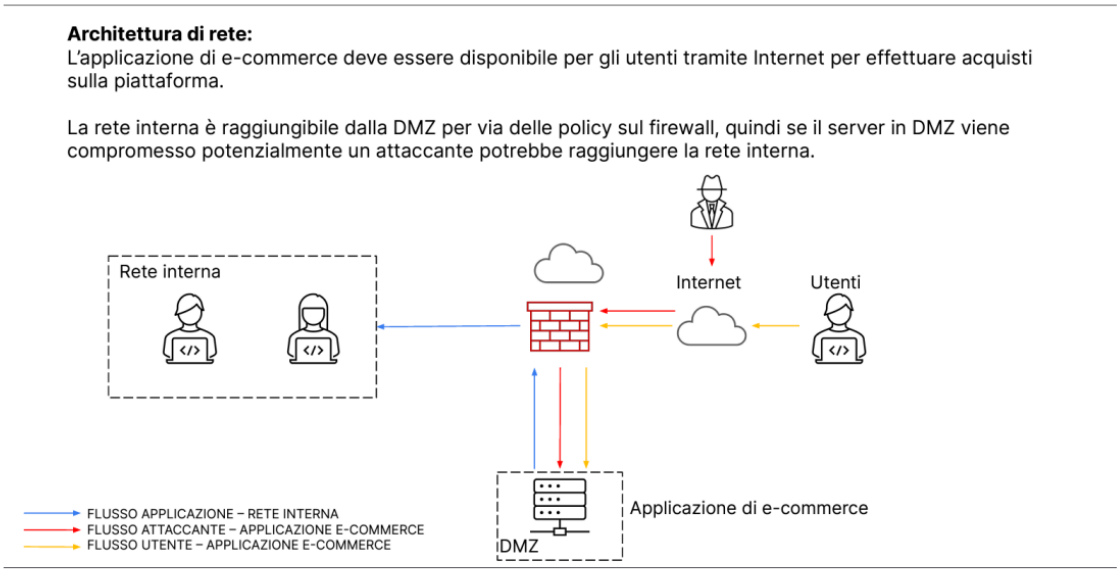
1. Azioni preventive: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni

2. 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. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica

3. 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.

4. Soluzione completa: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3

5. Modifica «più aggressiva» dell'infrastruttura (se necessario/facoltativo magari integrando la soluzione al punto 2



Studente: Isabelle Adjetey
Corso Cybersecurity & Ethical Hacking

Domanda 1

In caso di attacchi SQLi e XSS possiamo prevedere una serie di azioni mirate.

FILTRAGGIO DELLE CONNESSIONI in ingresso in modo da identificare e neutralizzare eventuali utenti malintenzionati.
Il filtraggio può avvenire tramite:

- WAF (Web Application Firewall) direttamente su web app
- IPS / IDS sull'intera rete

CONTROLLI SUL SOFTWARE

Per proteggere un'applicazione web da attacchi di tipo SQL Injection (SQLi) e Cross-Site Scripting (XSS), è fondamentale applicare una serie di azioni preventive. Alcune delle principali sono le seguenti:

1. **Aggiornamenti regolari**: Mantenere aggiornati tutti i software, inclusi framework e librerie, per proteggersi dalle vulnerabilità note.
2. **Test di sicurezza periodici**: Eseguire regolarmente delle penetration test e delle scansioni di vulnerabilità per identificare e correggere eventuali falle di sicurezza.
3. **Formazione del personale**: Assicurarsi che gli svillupatori siano formati sulle migliori pratiche di sicurezza e sulle tecniche di prevenzioni deli attachi.

In maniera più specifica, le misure che si possono addottare per proteggersi.

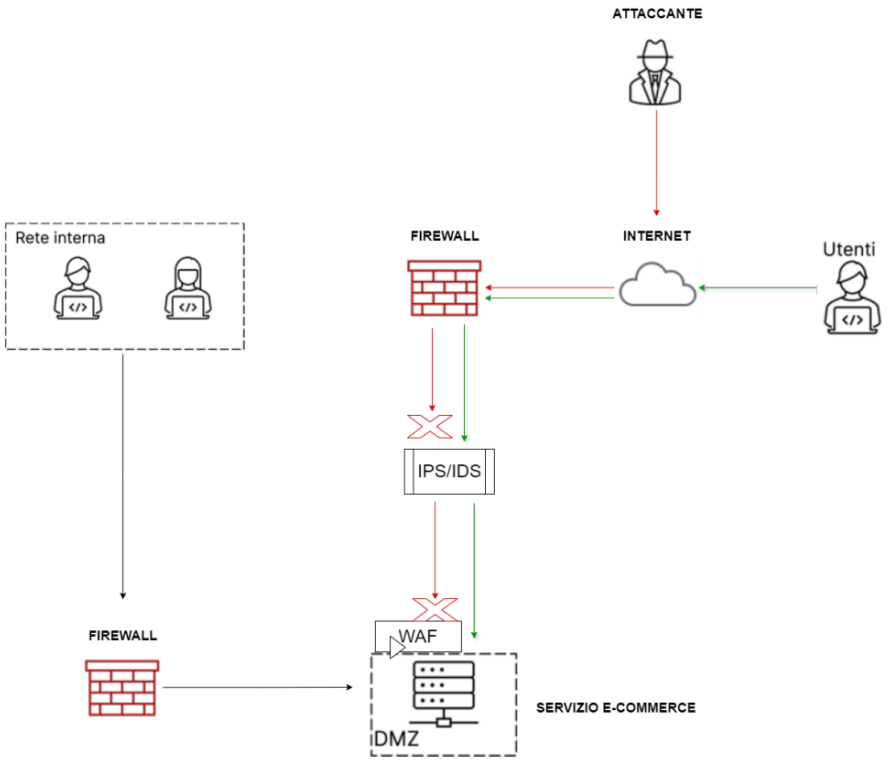
Contro SQL Injection (SQLi)

1. **Utilizzare query parametrizzate**: Assicurati che tutte le query SQL utilizzino parametri invece di concatenare direttamente i dati dell'utente. Questo impedisce agli attaccanti di inserire codice SQL malevolo.
2. **Validazione e sanificazione degli input**: Controllare e pulire tutti i dati in ingresso per assicurarti che non contengano caratteri o stringhe pericolose.
3. **Utilizzare ORM (Object-Relational Mapping)**: Gli ORM possono aiutare a prevenire SQLi automatizzando la gestione delle query SQL in modo sicuro.
4. **Configurare correttamente il database**: Limitare i permessi degli account del database utilizzati dall'applicazione, concedendo solo i privilegi necessari.

Contro Cross-Site Scripting (XSS)

1. **Sanificazione degli input e output**: Utilizzare funzioni di sanificazione per rimuovere o codificare i caratteri speciali dagli input dell'utente prima di renderizzarli nel browser.
2. **Content Security Policy (CSP)**: Implementare una CSP per limitare le fonti da cui il browser può caricare script, riducendo così il rischio di esecuzione di script malevoli.

3. **Evitare l'uso di** eval(): Non utilizzare eval() o altre funzioni simili che eseguono codice JavaScript dinamico, poiché possono essere sfruttate per eseguire codice malevolo.
4. **Utilizzare librerie di sicurezza**: Adottare librerie e framework che offrono protezioni integrate contro XSS, come Angular o React.



Nell'immagine sopra, è possibile vedere l'applicazione di WAF e sistemi IPS/IDS, che si interpongono tra la web app e l'attaccante, e un firewall ad hoc per la rete interna, per limitare il traffico di eventuali agenti esterni non autorizzati.

Domanda 2

1. **Calcolo della perdita di entrate**:
   - Se gli utenti spendono in media 1.500 € al minuto sulla piattaforma di e-commerce, la perdita totale in 10 minuti sarà:

     Impatto sull'attività = Valore medio generato dagli utenti per minuto* Numero di minuti di indisponibilità

     Impatto sull'attività = 1.500€×10minuti=15.000€

Quindi, l'impatto economico dell'attacco DDoS è di 15.000 €

2. **Valutazioni di azioni preventive**:

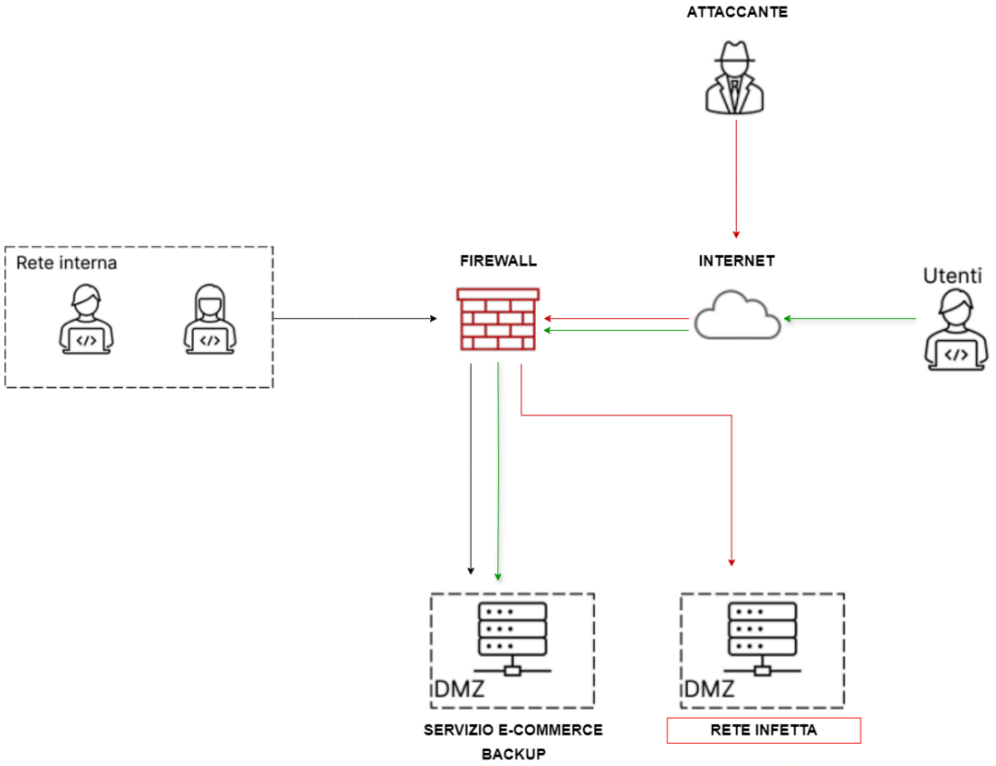
Utilizzo di un Web Application Firewall (WAF) per filtrare e mitigare il traffico DDoS in arrivo.

- **Implementazione di soluzioni anti-DDoS**: Utilizzare servizi di mitigazione DDoS che possono rilevare e bloccare il traffico malevolo prima che raggiunga il server (Utilizzo di un Web Application Firewall (WAF) per esempio?
- **Ridondanza e bilanciamento del carico**: Distribuire il traffico su più server per evitare che un singolo punto di guasto possa rendere l'intera applicazione non raggiungibile.
- **Monitoraggio continuo**: Implementare sistemi di monitoraggio per rilevare tempestivamente attività sospette e rispondere rapidamente agli attacchi.
- **Piani di risposta agli incidenti**: Avere un piano dettagliato per rispondere agli attacchi DDoS, inclusi contatti di emergenza e procedure di ripristino.

Domanda 3

In questo caso, se esiste un backup della web app, si protrebbe indirizzare il traffico dell'agente attaccante sulla rete/db che è già stata infettata, limitando lì la sua presenza. Sul secondo server, quello di backup, avverrà invece il normale traffico previsto, ovvero le connessioni della rete interna e quelle degli utenti che devono usufruire dei servizi dell'ecommerce. Il firewall, in pratica, se correttamente impostato, permetterebbe lo smitamento delle connessioni in entrata automaticamente verso il server infetto per gli agenti malevoli e verso il server di backup per gli agenti autorizzati.

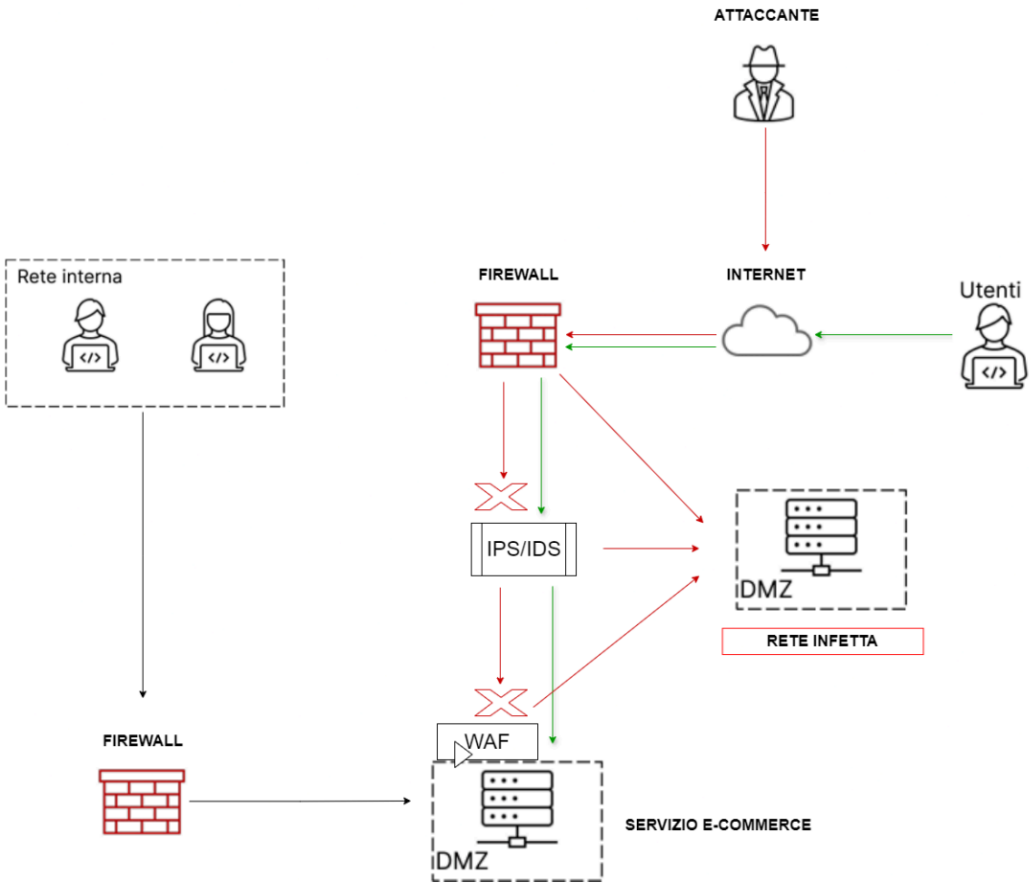
Studente: Isabelle Adjetey
Corso Cybersecurity & Ethical Hacking



Domanda 4

Lo schema sottostante fa vedere le misure preventive introdotte nel prima doman da e la soluzione alla terza domanda

Studente: Isabelle Adjetey
Corso Cybersecurity & Ethical Hacking



Domanda 5

La modifica più aggressiva sarebbe quella di isolare completamente la rete infetta, bloccando qualsiasi tipo di connessione.

Studente: Isabelle Adjetey
Corso Cybersecurity & Ethical Hacking