PROGETTO

Indice:

Risoluzione:

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

Per difendere le web application da attacchi di tipo SQLi (iniezione di codice SQL) e XSS (Cross-site Scripting), è fondamentale adottare misure preventive e difensive. Ecco alcune azioni consigliate:

1. Validazione degli input: Assicurarsi che tutti gli input forniti dagli utenti siano correttamente validati. Questo significa controllare che i dati inseriti nei form siano conformi alle aspettative e non contengano codice malevolo.
2. Tecniche di isolamento: Utilizzare tecniche di isolamento per prevenire attacchi di tipo injection. Ad esempio, utilizzare statement parametrizzati, escape degli input dell'utente e validazione degli input.
3. Implementare un firewall per applicazioni web (WAF): Un WAF è una tecnologia che filtra il traffico HTTP/HTTPS tra gli utenti e l'applicazione web. Questo aiuta a rilevare e bloccare attacchi comuni come SQLi e XSS. Il WAF può essere configurato per filtrare il traffico in base a regole specifiche e proteggere l'applicazione da vulnerabilità note.

4. Aggiornare regolarmente il software: Mantenere il software dell'applicazione web aggiornato con le ultime patch di sicurezza. Questo riduce le vulnerabilità note e protegge l'applicazione da attacchi noti.
5. Educazione degli utenti: Sensibilizzare gli utenti riguardo alle minacce informatiche. Insegnare loro a riconoscere segni di attacchi e a utilizzare l'applicazione in modo sicuro.
6. Backup regolari: Effettuare backup regolari dei dati dell'applicazione. In caso di attacco, è possibile ripristinare i dati da un backup sicuro.
7. Monitoraggio costante: Monitorare costantemente l'applicazione per rilevare eventuali anomalie o attività sospette. Utilizzare strumenti di monitoraggio e log per identificare potenziali attacchi.
8. Test di sicurezza: Effettuare test di sicurezza regolari per identificare vulnerabilità nell'applicazione. Questi test possono essere manuali o automatizzati e aiutano a individuare potenziali problemi di sicurezza.

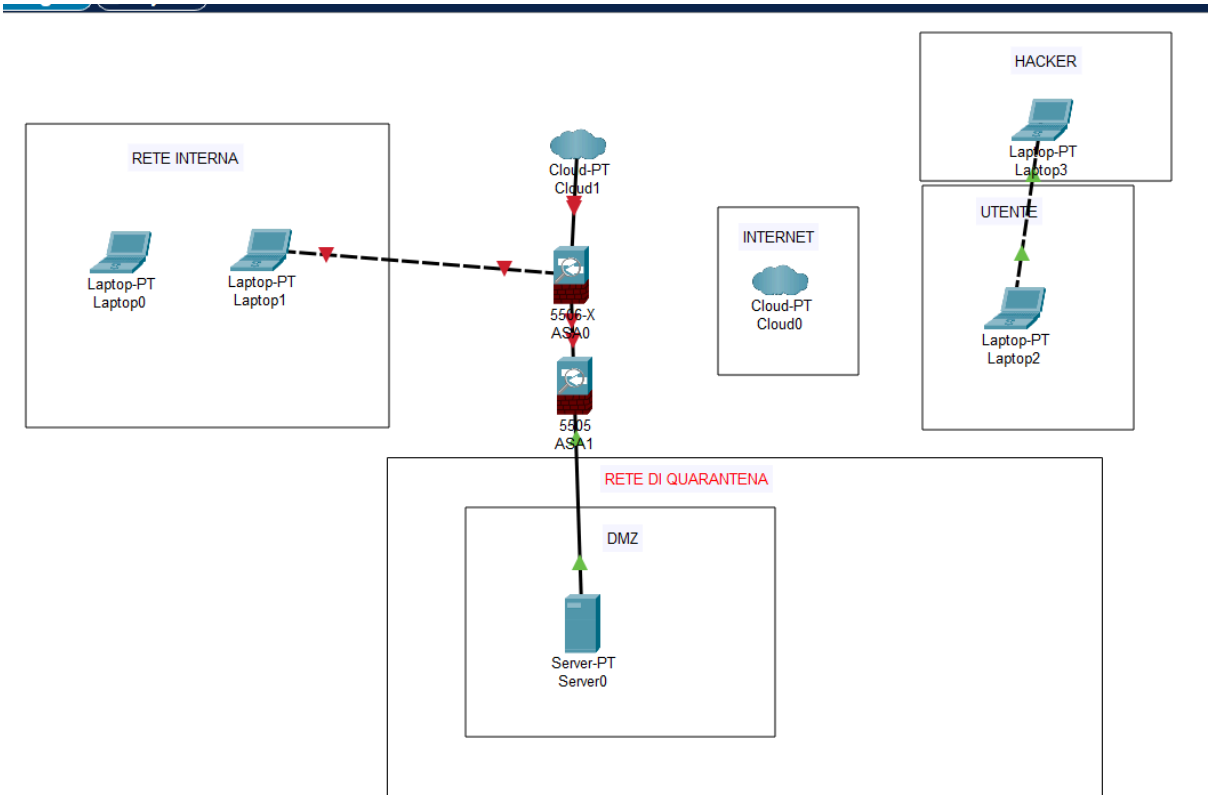
   2) Response: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostre rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.

1. Identificare il problema: Il primo passo è capire che c'è un problema. Questo potrebbe includere segnali di avvertimento come prestazioni lente, crash frequenti o messaggi di errore inaspettati.
2. Isolare la macchina infettata: Per prevenire la diffusione del malware, dovresti isolare la macchina infettata dal resto della rete.
3. Rimuovere il malware: Dopo aver messo il sistema in rete di quarantena, bisogna rimuovere la macchina infettata dalla rete per poi procedere con Purge che è un approccio si adottano

sia misure logiche che misure fisiche per l'eliminazione permanente dei dati su un disco / dispositivo di storage. Le tecniche fisiche utilizzate tuttavia non sono invasive, e non implicano la distruzione dell'hardware, o Destroy utilizza tecniche fisiche molto invasive per rendere inaccessibili i dati su un disco / dispositivo di storage. Alcune delle tecniche prevedono la distruzione a livello di hardware di fatto rendendo non recuperabile l'hardware e le relative informazioni salvate su di esso. È il metodo preferito quando si vuole smaltire un disco non riutilizzabile, ma è anche quello che costa di più.

4. Ripristinare i file infetti: Se i file sono stati danneggiati o modificati dal malware, potrebbe essere necessario ripristinarli da un backup.
5. Aggiornare e patchare il sistema: Dopo aver rimosso il malware, dovresti assicurarti che il tuo sistema sia aggiornato con le ultime patch di sicurezza. Questo può aiutare a prevenire future infezioni.
6. Monitorare il sistema: Dopo aver ripulito il malware, dovresti continuare a monitorare il sistema per qualsiasi segno di attività sospetta.

Nel diagramma che segue, ho implementato un Firewall per Applicazioni Web (WAF) subito dopo il firewall principale. Questo serve a proteggere l'applicazione web da potenziali minacce esterne. Se l'applicazione web dovesse essere compromessa da un malware, la procedura consigliata sarebbe di isolare l'applicazione web all'interno di una rete di quarantena. In questo modo, l'attaccante avrebbe accesso solo al sistema infetto attraverso internet. Successivamente, procederemo con la disconnessione dell'applicazione web da internet, impedendo così all'attaccante di accedere ulteriormente alla macchina infettata. Infine, metteremo in atto i meccanismi di "purge" o "destroy".



3) 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

ALE (Annualised loss expectancy) = SLE x ARO

ALE = 1.500 x 10 = € 15.000

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, è di €15.000.

4) Per quanto riguarda le azioni preventive che si possono applicare in questa problematica, ecco alcune possibili soluzioni:

1. **Adottare un servizio di mitigazione DDoS**: Questi servizi possono rilevare e respingere gli attacchi DDoS prima che raggiungano la tua applicazione.

2. **Avere una capacità di banda in eccesso**: Questo può aiutare a gestire l'aumento del traffico durante un attacco DDoS.
3. **Utilizzare un sistema di prevenzione delle intrusioni (IPS)**: Questi sistemi possono identificare e bloccare gli attacchi DDoS.
4. **Implementare la ridondanza del server**: Avere più server in diverse posizioni geografiche può aiutare a garantire che se un server viene attaccato, gli altri possono continuare a funzionare.
5. **Creare un piano di risposta agli incidenti**: Avere un piano in atto può aiutare a minimizzare il danno quando si verifica un attacco.