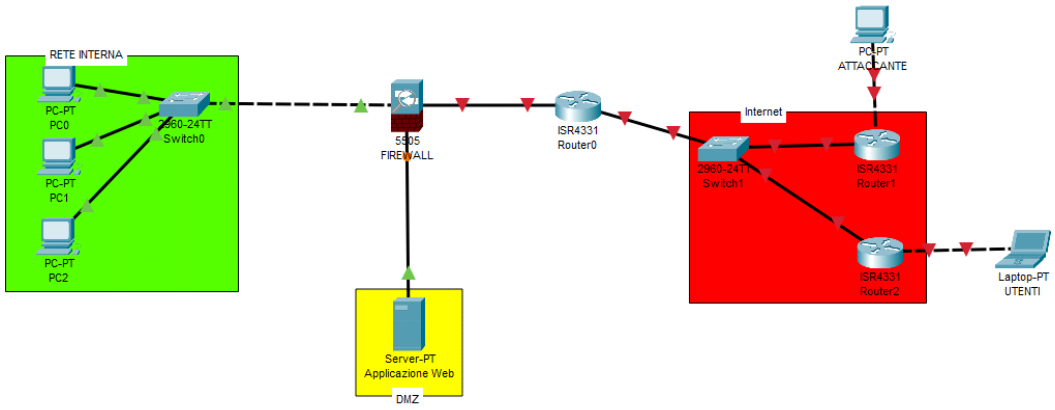
Progetto
24/03/2023



Azioni preventive

Per difendere l'applicazione Web da attacchi di tipo SQLi e XSS, si possono implementare le seguenti azioni preventive:

1. Utilizzo di un WAF (Web Application Firewall): è un tipo di firewall progettato specificamente per proteggere le applicazioni web. Un WAF funziona come un filtro tra il server web e il traffico Internet, analizzando il traffico HTTP/HTTPS in entrata e in uscita per identificare e bloccare le potenziali minacce alla sicurezza.

2. Validazione dei dati in input: tutti i dati inseriti dall'utente devono essere validati, filtrati e sanificati, in modo da evitare l'inserimento di dati malevoli. (Osservare inoltre che i dati rispettino il formato corretto e che siano conformi alle regole di business).

3. Utilizzo di parametri preparati per le query SQL: evita di creare query SQL dinamiche concatenando i dati di input. Utilizza invece parametri nelle query SQL in modo che i dati di input non possano essere interpretati come codice SQL.

4. Utilizzo di librerie e framework sicuri: utilizza librerie e framework sicuri che supportano la prevenzione di attacchi XSS e SQLi. Queste librerie spesso forniscono funzioni di validazione dei dati di input e di parametrizzazione delle query SQL.

5. Filtro dei dati di input: filtra i dati di input per rimuovere caratteri speciali e codice HTML. Ciò può impedire l'esecuzione di script dannosi e l'inserimento di codice SQL dannoso.

6. Utilizzo di HTTPS: utilizza HTTPS per cifrare la comunicazione tra il browser dell'utente e il server web. Questo impedirà che gli attaccanti intercettino i dati sensibili.

7. Utilizzo di token CSRF: i token CSRF (Cross-Site Request Forgery) vengono utilizzati per

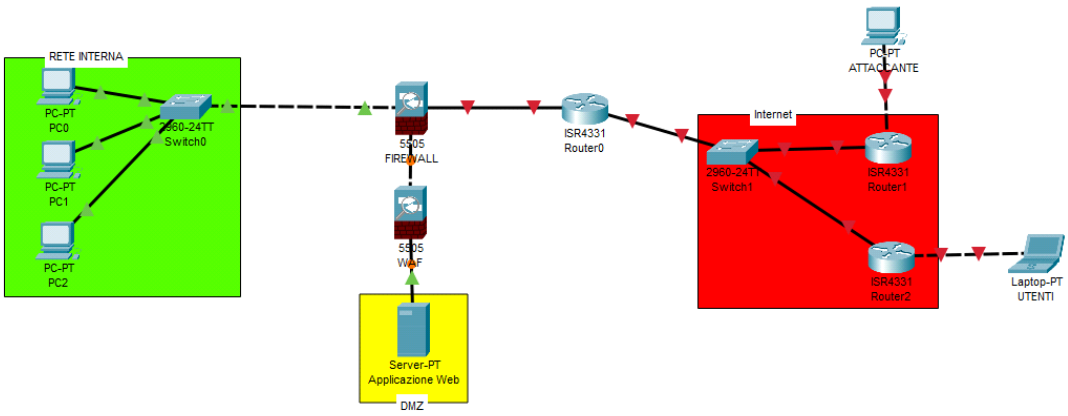
evitare che un attaccante possa sfruttare la sessione di un utente per eseguire azioni malevole.

8. Una Content Security Policy (CSP): può aiutare a mitigare gli attacchi XSS specificando quali risorse (script, stili, immagini, ecc.) possono essere caricate.

9. Controllo degli accessi: implementare controlli di accesso per limitare l'accesso ai dati sensibili. In questo modo, solo gli utenti autorizzati possono accedere ai dati.

10. Aggiornamenti regolari: mantenere il software e le librerie sempre aggiornati con le ultime patch di sicurezza. Ciò può prevenire l'exploit di vulnerabilità note.

11. Test di sicurezza: eseguire regolarmente test di sicurezza sull'applicazione per identificare e correggere eventuali vulnerabilità. Ciò può impedire che gli attaccanti sfruttino le vulnerabilità per eseguire attacchi XSS o SQLi.



Impatto sul business

A seguito di un attacco DDoS dall'esterno, che ha reso l'applicazione non raggiungibile per 10 minuti, ho calcolato l'impatto sul business considerando che in media ogni minuto gli utenti spendono 1.500 € sulla piattaforma di e-commerce.

Impatto totale = 10 minuti * 1.500 €/minuto = 15.000 €

Azioni preventive per far fronte alle perdite economiche:

1. Utilizzo di sistemi IPS e IDS: Per proteggere la struttura di rete da attacchi di tipo DDoS.

2. Riduzione del traffico in entrata: implementa un sistema per ridurre il traffico in entrata, ad esempio mediante la limitazione del numero di richieste da un determinato indirizzo IP.

3. Configurazione del firewall: configura il firewall per bloccare il traffico proveniente da fonti sospette e limitare l'accesso ai servizi web solo ai clienti autorizzati.

4. Miglioramento della capacità del server: ciò può essere fatto utilizzando server con maggiore capacità di elaborazione e connessioni di rete più veloci.

5. Utilizzo di servizi di hosting sicuri: assicurati di utilizzare un servizio di hosting sicuro che disponga di meccanismi di sicurezza robusti per proteggere il tuo sito web.

6. Creazione di un sito mirror: una copia del sito, che sarà operativa in caso di immobilizzazione della piattaforma originale.

7. Aggiunta di un failover cluster: prevede l'utilizzo di più server replicati in modo da garantire la continuità del servizio in caso di interruzione.In questo modo se uno dei server cluster viene colpito gli altri server possono continuare a gestire il carico di lavoro.

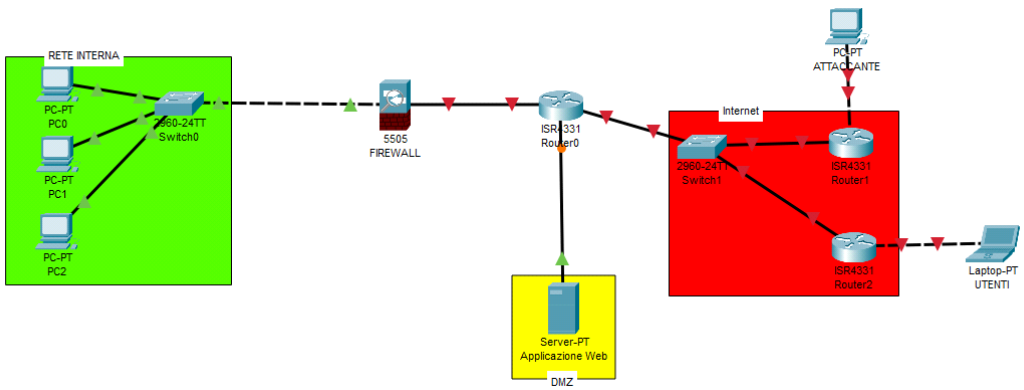
8. Utilizzo di servizi cloud: per distribuire il traffico e prevenire un'interruzione del servizio in caso di attacco DDoS.

9. Sovrastima delle necessità: effettuando una stima in eccesso delle risorse che saranno necessarie a un determinato sistema informatico, si sarà cosi in grado di fronteggiare attacchi che puntano a saturare la banda o la capacità di calcolo di un server o di un centro dati.

10. Aggiornamento regolare del software: mantenere il software del sito web sempre aggiornato con le ultime patch di sicurezza per prevenire eventuali vulnerabilità note che potrebbero essere sfruttate in un attacco DDoS.

11. Pianificazione di un piano di emergenza: pianificare un piano di emergenza in caso di attacco DDoS per essere preparati ad affrontare l'attacco e ripristinare il servizio il prima possibile.

Response



Per evitare che il malware si propaghi sulla nostra rete possiamo:

1. Isolare immediatamente la macchina infetta: è importante limitare l'accesso della macchina infetta alla rete interna per prevenire la propagazione del malware. In questo caso, potrebbe essere necessario limitare l'accesso solo alla rete DMZ, impedendo l'accesso ad altre parti della rete interna.

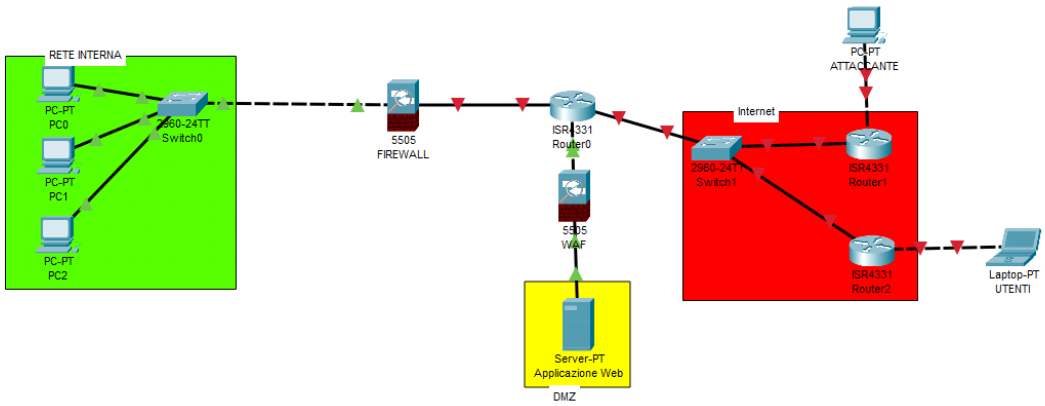
2. Analisi del malware: una volta isolata la macchina infetta, si dovrebbe procedere all'analisi del malware per capire come è entrato e quali sono i danni che ha causato. Questo aiuterà a prendere decisioni informate su come procedere.

3. Rimozione del malware: una volta che il malware è stato analizzato, viene rimosso dalla macchina infettata.

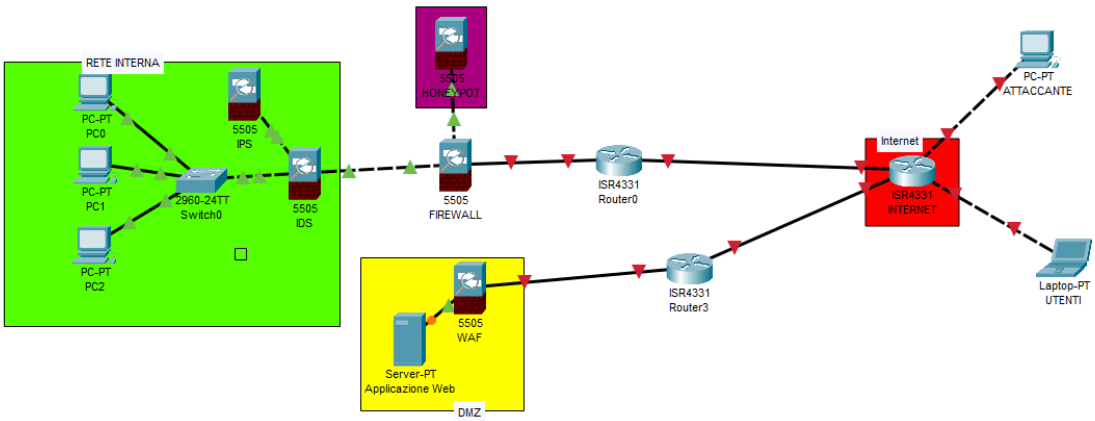
4. Pulizia e ripristino: infine, sarà necessario procedere alla pulizia della macchina infetta e al ripristino della sua configurazione precedente per evitare ulteriori danni.

5. Patching del sistema: è una pratica comune e importante per garantire la sicurezza informatica e migliorare la stabilità e le funzionalità del sistema.

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



Modifica "più aggressiva" dell'infrastruttura



IPS: è un sistema di sicurezza informatica che monitora il traffico di rete in cerca di eventuali intrusioni o attività sospette e agisce per prevenire attivamente tali attacchi. In altre parole, l'IPS è un sistema di rilevamento e prevenzione delle intrusioni in grado di monitorare il traffico di rete, rilevare attività sospette e bloccare eventuali tentativi di intrusione.

IDS: funziona monitorando il traffico di rete in tempo reale, alla ricerca di eventuali attività sospette o comportamenti anomali, che potrebbero indicare un attacco in corso.

Honeypot: può essere utilizzato per rilevare e raccogliere informazioni sulle tecniche di attacco utilizzate dagli hacker, sui tipi di malware impiegati e sulla loro origine geografica. Inoltre, l'utilizzo di honeypot può fornire un'opportunità per gli amministratori di sistema di testare e migliorare le loro difese informatiche e di prevenire futuri attacchi.