W20D4

Azioni Preventive

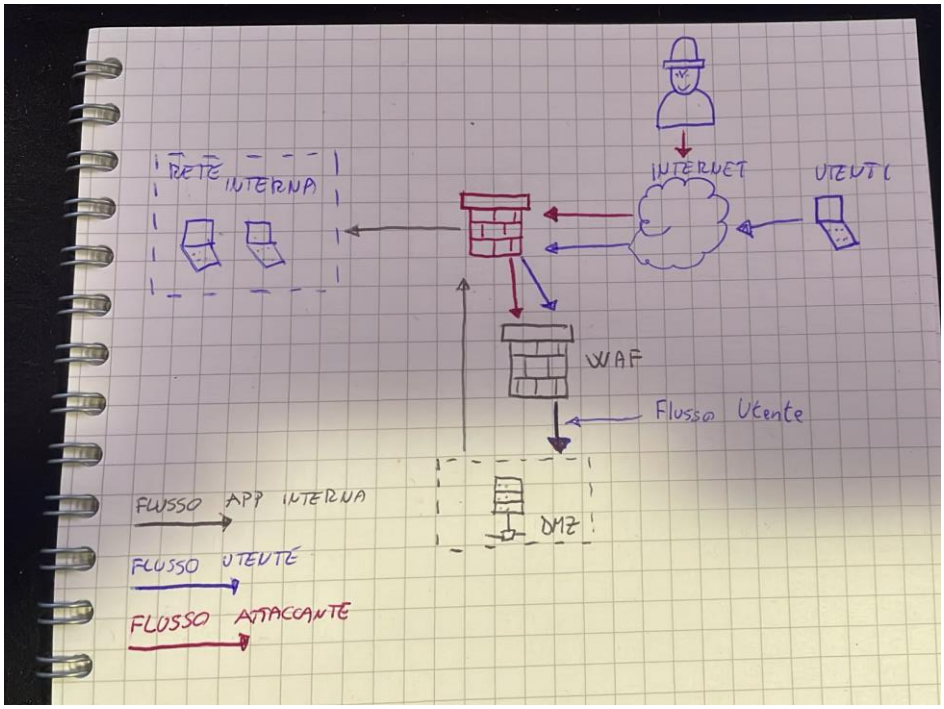
TRACCIA PUNTO 1

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

SOLUZIONE PUNTO 1

Per proteggere il server sul quale vi è hostata la nostra web app da attacchi di tipo SQLi oppure XSS da parte di un eventuale malintenzionato, dovremmo inserire tra il nostro Firewall base un Firewall di tipo WAF, il quale si differenzia dai Firewall normali perché essi sono proprio dedicati alla protezione delle Web App dalle tipologie di attacchi sopra citati. Tramite il Waf potremo creare delle regole molto più stringenti per evitare eventuali accessi indesiderati o tentativi di attacchi al server.

FIGURA MODIFICATA



Impatti sul Business

TRACCIA PUNTO 2

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

SOLUZIONE PUNTO 2

L’attacco di tipo DDoS consiste nel saturare un server effettuando un invio massiccio di pacchetti o richieste, il quale non essendo in grado di gestire tutte le richieste inviate potrebbe creare delle vulnerabilità poi da sfruttare, oppure potrebbe crashare bloccando così come da esempio un servizio che fa perdere danari all’azienda che usufruisce di quel servizio.

Nella traccia possiamo notare come questo attacco ha un impatto sul business di 1.500€ al minuto il che vuol dire che in 10 minuti si perdono 15.000€

10x 1.500€ = 15.000€

L’azienda avendo un down di questo servizio per 10minuti andrebbe a perdere un somma di € 15k

Per evitare eventuali attacchi DDoS si possono implementare delle regole a monte fin dal router ma anche all’interno del firewall, vi sono delle regole che permettono di limitare quanti pacchetti un utente può inviare in un tot di secondi, quando l’utente supere i pacchetti inviati in un tot di secondi i successivi vengono droppati così che il dispositivo che hosta la WebApp non riceva questi pacchetti e non vada in Crash o si blocchi per le troppe richieste.

Queste regole molte volte sono anche attivabili molto velocemente perché già preimpostate dal costruttore degli apparati di rete

Response

TRACCIA PUNTO 3

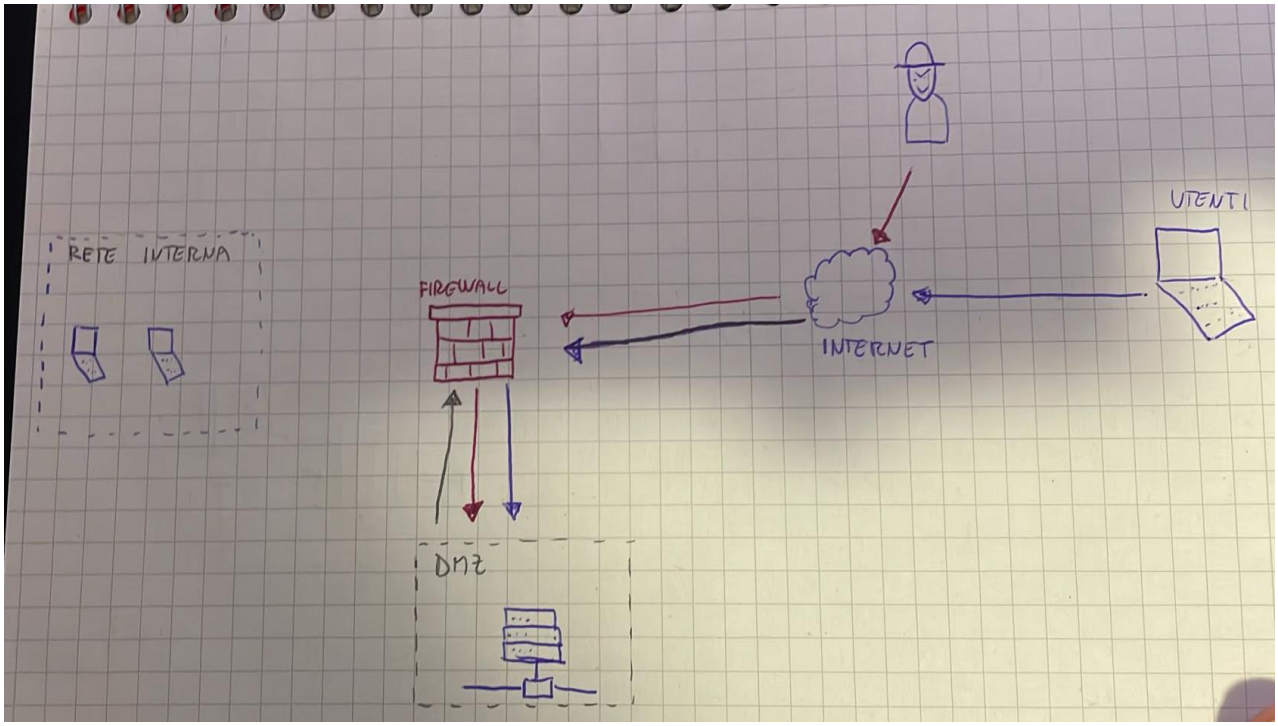
l’applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l’accesso da parte dell’attaccante alla macchina infettata. Modificate la figura in slide 2 con la soluzione proposta.

SOLUZIONE PUNTO 3

Data la priorità della situazione si può intraprendere una via di isolamento della macchina infetta, in questo caso creeremo delle regole dedicate per il firewall, in modo tale che la macchina possa ricevere comunicazione dall’esterno ma che quest’ultima non possa comunicare verso le macchine presenti nella nostra rete interna, così facendo l’hacker riuscirà a raggiungere la macchina da remoto ma non potrà propagare il suo virus oppure prendere il controllo di un'altra macchina.

Un’altra possibilità sarebbe quella di isolare direttamente la macchina infetta sia per comunicazioni dall’esterno che verso l’esterno, così facendo noi potremmo agire indisturbati per recuperare la macchina e renderla nuovamente sicura, evitando che il malintenzionato continui a modificare o a creare maggiori danni su di essa.

MAPPA PUNTO 3



Soluzione Completa

TRACCIA PUNTO 4

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

SOLUZIONE PUNTO 4: