Esercizio S9-L5

Traccia:

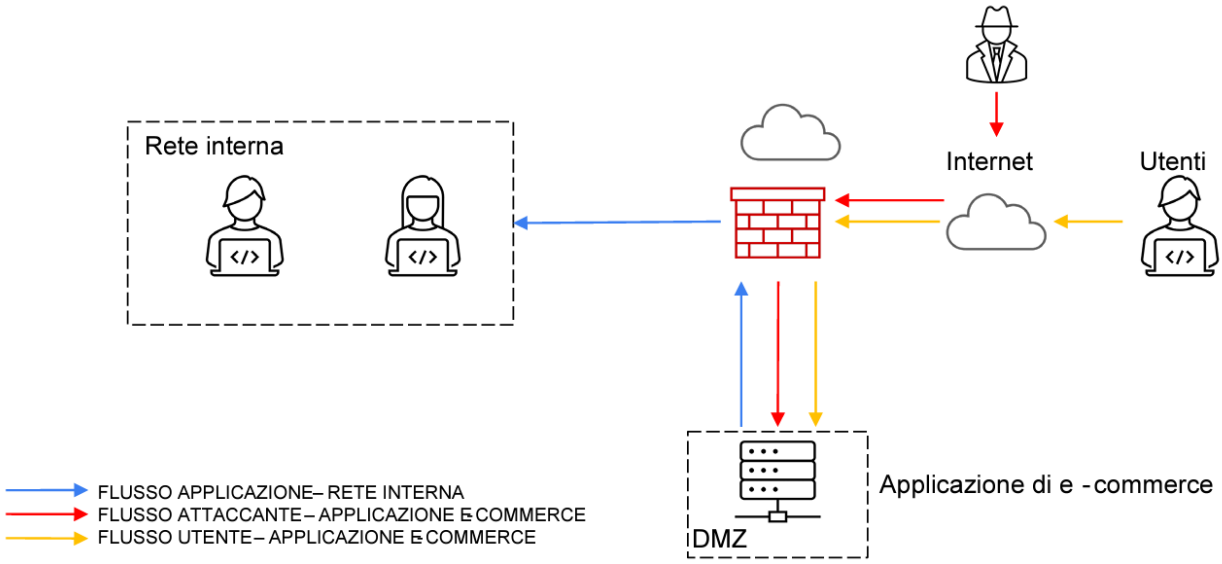
Azioni preventive: Quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi o XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni.

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.

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

Modifica "più aggressiva" dell'infrastruttura: Integrando eventuali altri elementi di sicurezza (se necessario/facoltativo magari integrando la soluzione al punto 2).



Esercizio S9-L5

Azioni preventive:

Per difendere un'applicazione web da attacchi SQLi o XSS, si possono implementare le seguenti misure:

Validazione dell'input: Assicurarsi che tutti gli input dell'utente siano validati prima di essere elaborati.

Parametri delle query: Utilizzare query parametrizate per prevenire l'iniezione di codice SQL malevolo.

Impatti sul business:

Se l'applicazione web non è raggiungibile per 10 minuti e in media ogni minuto gli utenti spendono 1.500 €, **l'impatto** economico sarebbe di **15.000 €** (10 minuti x 1.500 €/minuto).

Per prevenire attacchi DDoS, si potrebbe ricorrere a servizi di mitigazione DDoS o l'uso di CDN per distribuire il traffico.

Response:

Se l'applicazione web viene infettata da un malware, la priorità è quella di **isolare il web server** per prevenire la propagazione del malware sulla rete.

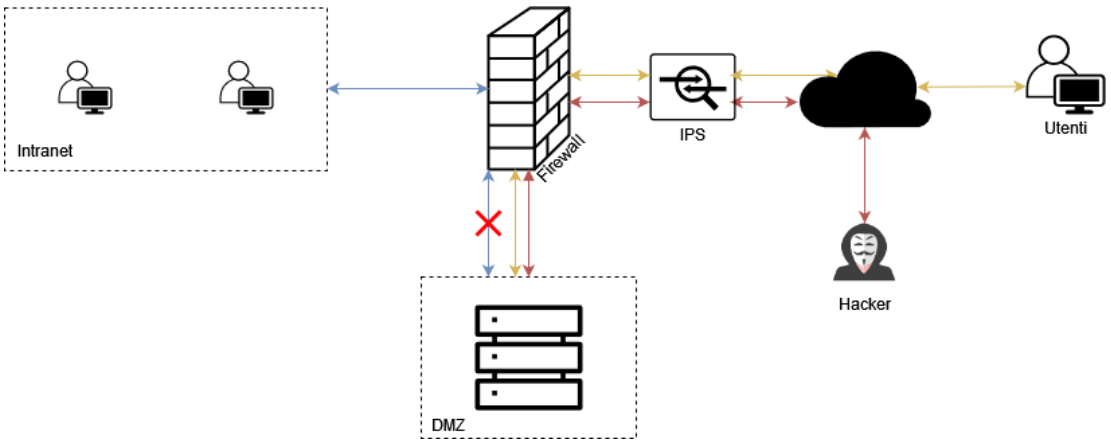
Lo andremo ad isolare dalla rete interna **bloccando l'interfaccia di rete del firewall che collega la DMZ alla rete Intranet.**

Soluzione completa:

La soluzione completa include sia le azioni preventive che le misure di risposta. Questo comporta l'implementazione di misure di sicurezza come la validazione dell'input, l'uso di policy di sicurezza, l'isolamento di applicazioni infette, e l'uso di servizi di mitigazione DDoS.

Modifica dell'infrastruttura:

Per una protezione ancora maggiore oltre all'IPS e all'isolamento, si potrebbero inserire ulteriori dispositivi di sicurezza, come un **Web Application Firewall**, una raccolta di log effettuata da un sistema **SIEM** o l'implementazione di un **SOC** per monitorare e rispondere alle minacce in tempo reale.



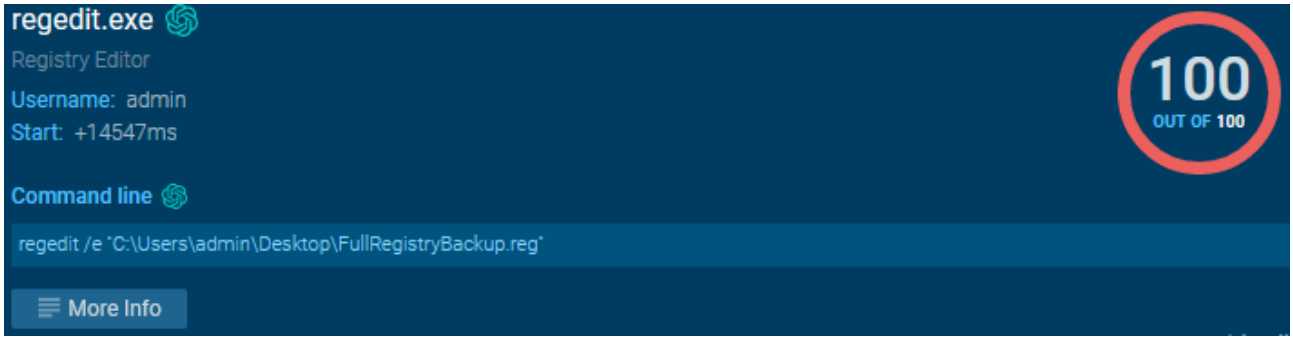
Esercizio S9-L5

Report aggiuntivi:

PERFORMANCE_BOOSTER_v3.6.exe:

Il file è malevolo e le task sospette includono l'esecuzione di script PowerShell e la lettura delle chiavi del registro di Microsoft Office.

Prove:



https://1drv.ms/u/s!At7eQ7h8kx6-nQM1RTCuz3aQspOE:

Come si può notare dal link si tratta di un collegamento malevolo che porta ad installare un finto **MicrosoftEdgeUpdate.exe**

Prove: