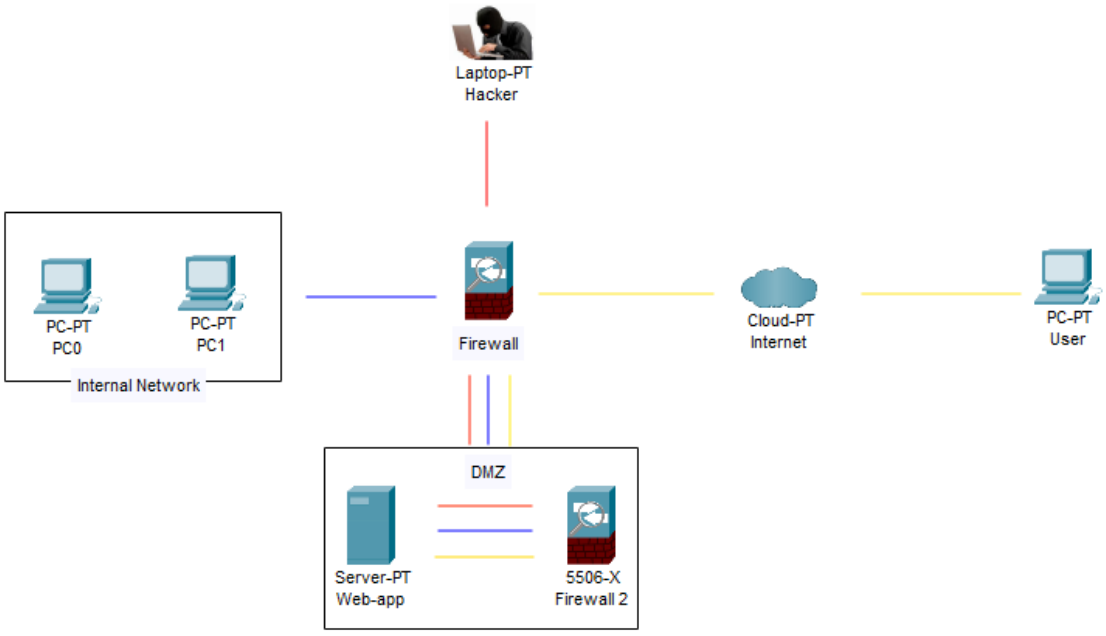
# ANALISI DEI LOG – CASO REALE

**Scopo dell'esercizio:**

Gentile prof, L'obiettivo di questo esercizio è valutare la sicurezza dell'applicazione Web e identificare le potenziali vulnerabilità che potrebbero consentire attacchi di tipo SQLi (Injection SQL) o XSS (Cross-Site Scripting) da parte di utenti malevoli. Saranno esaminate anche le azioni preventive da implementare e le soluzioni per rispondere a una possibile infezione da malware.

**Azioni preventive:**




Per difendere l'applicazione Web da attacchi di tipo SQLi e XSS, è possibile implementare le seguenti azioni preventive:
Validazione dei dati in ingresso: Validare accuratamente i dati immessi dagli utenti per rilevare eventuali caratteri o sequenze sospette che potrebbero essere utilizzate per eseguire attacchi di tipo SQLi o XSS.
Parametrizzazione delle query SQL: Utilizzare parametri nelle query SQL per evitare l'inserimento diretto di valori immessi dagli utenti, riducendo così il rischio di SQLi.
Filtro e sanitizzazione degli input: Applicare filtri e sanitizzazioni ai dati in ingresso per rimuovere o neutralizzare eventuali caratteri pericolosi o codice maligno che potrebbero causare attacchi XSS.

Protezione contro l'esecuzione di script non autorizzati: Implementare meccanismi di protezione come l'HTML encoding per evitare l'esecuzione di script non autorizzati all'interno delle pagine Web.
Aggiornamento regolare delle librerie e dei framework: Mantenere aggiornate le librerie e i framework utilizzati nell'applicazione per beneficiare delle correzioni di sicurezza più recenti.

**Azioni preventive implementate:**

Nella figura in Slide 2, sono state evidenziate le seguenti implementazioni delle azioni preventive:

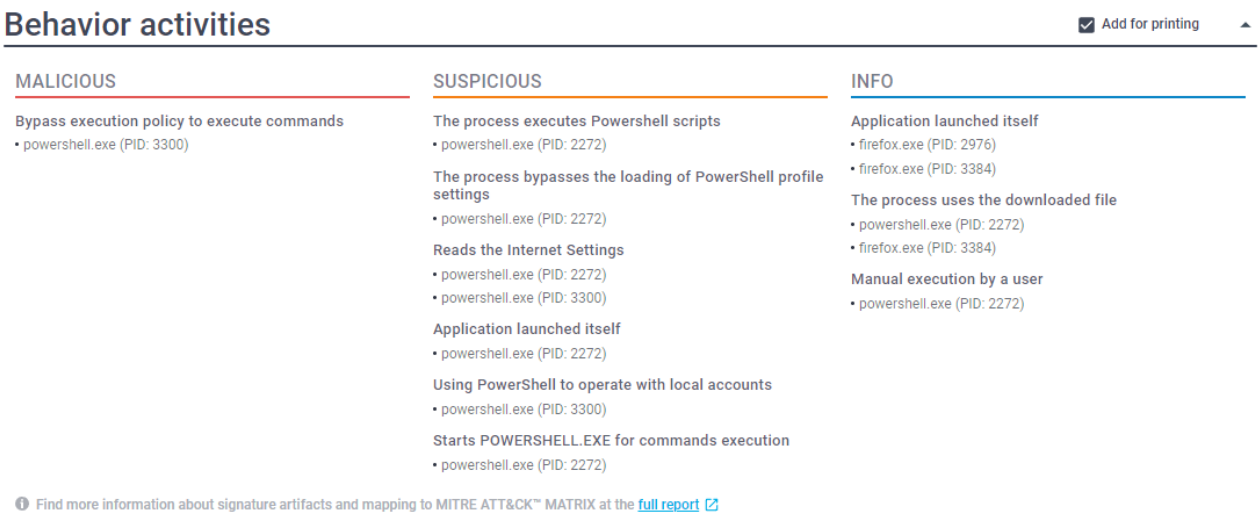
Validazione dei dati in ingresso con sanitizzazione per prevenire attacchi SQLi e XSS.
Parametrizzazione delle query SQL per evitare l'inserimento diretto di valori immessi dagli utenti.
Filtro e sanitizzazione degli input per rimuovere o neutralizzare caratteri pericolosi o codice maligno.
Protezione contro l'esecuzione di script non autorizzati mediante l'HTML encoding.
Aggiornamento regolare delle librerie e dei framework utilizzati nell'applicazione.

**Analisi attacco:**

Sono stati forniti due link da analizzare:

**Link sospetto 1: https://tinyurl.com/linklosco1**
**Link sospetto 2: https://tinyurl.com/linklosco2**

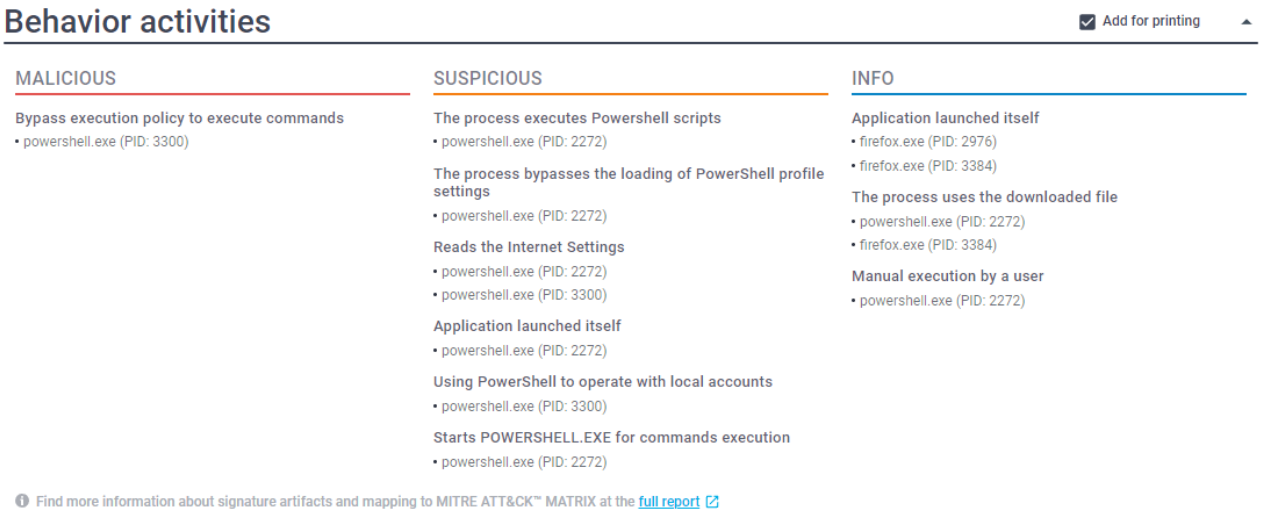
Sulla base dell'analisi dei link, sono state riscontrate le seguenti informazioni:




**Link sospetto 1/Attività sospette:**

Bypass execution policy to execute commands: Il processo "powershell.exe" con PID 3300 ha bypassato la politica di esecuzione per eseguire comandi. Questa azione potrebbe indicare un tentativo di eseguire comandi maligno compromettenti utilizzando PowerShell.

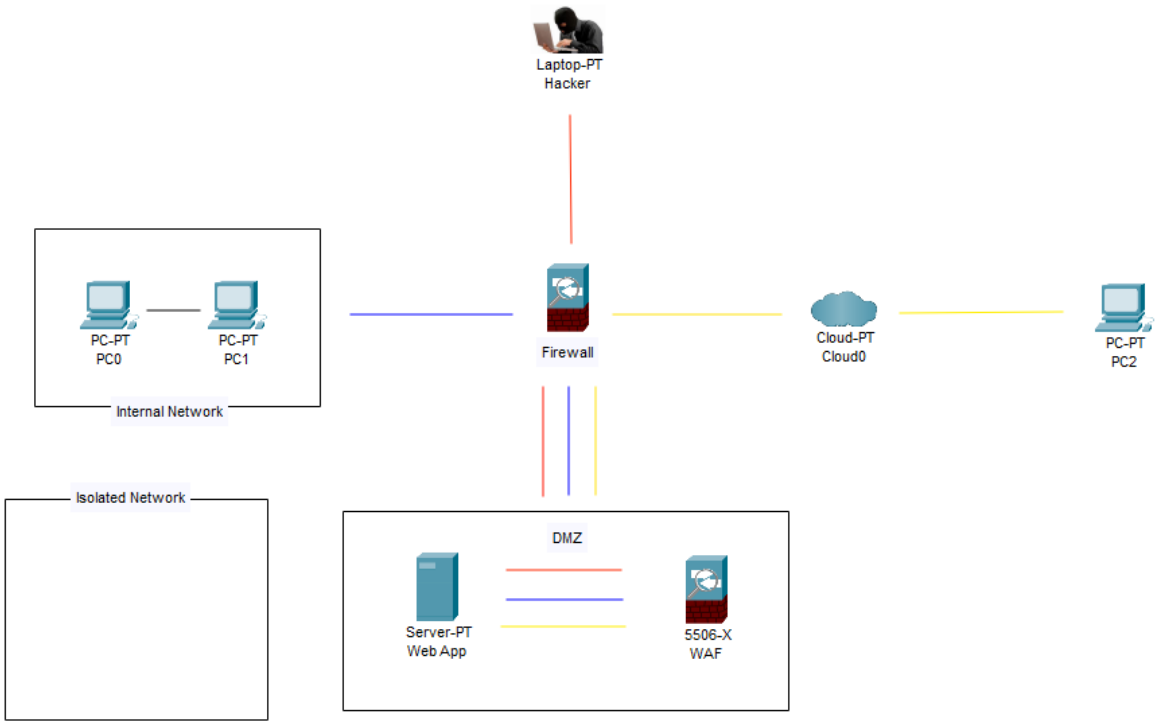
The process executes Powershell scripts: Il processo "powershell.exe" con PID 2272 ha eseguito script PowerShell. Questo comportamento può essere sospetto e potenzialmente indicare un utilizzo di PowerShell per scopi malevoli.

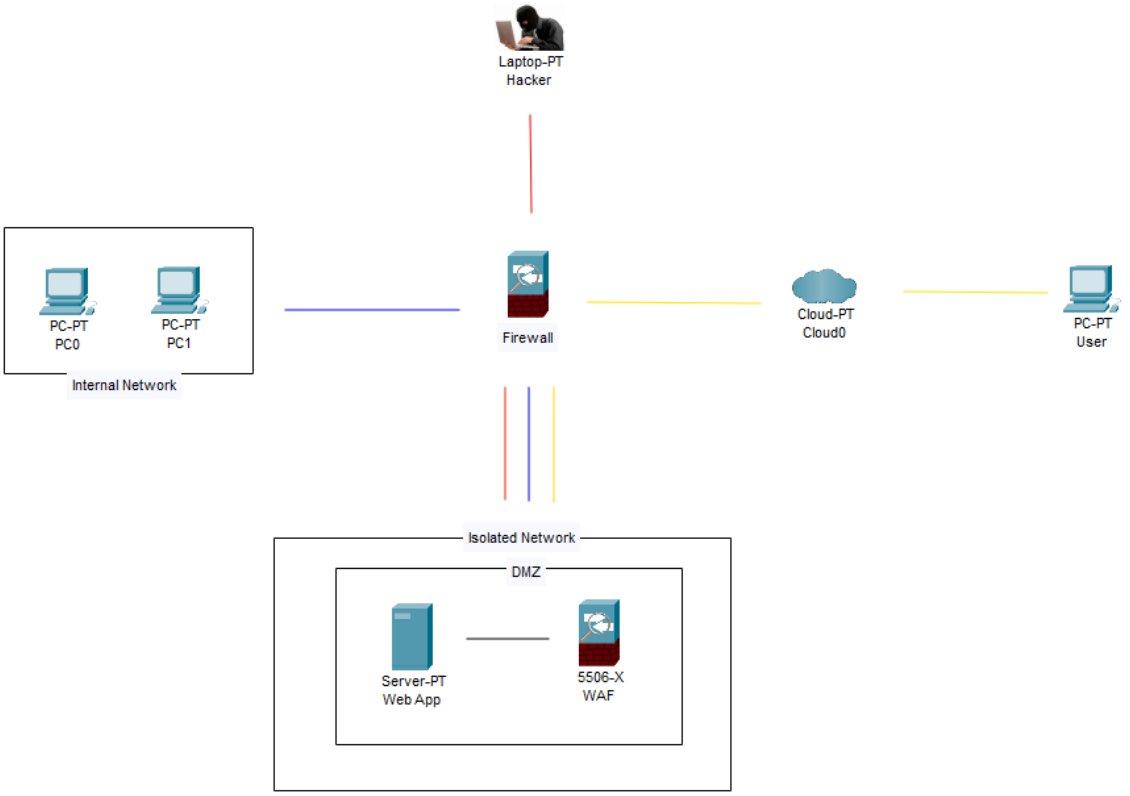


**Link sospetto 2/Attività sospette:**

Application launched itself: Il processo "firefox.exe" con PID 2976 ha avviato se stesso. Questa azione potrebbe indicare un comportamento anomalo o un tentativo di eseguire un'operazione non autorizzata.
The process bypasses the loading of PowerShell profile settings: Il processo "firefox.exe" con PID 3384 ha bypassato il caricamento delle impostazioni del profilo di PowerShell. Questo comportamento potrebbe indicare un tentativo di evitare la rilevazione o di eseguire operazioni non autorizzate utilizzando PowerShell.
The process uses the downloaded file: Sia il processo "powershell.exe" con PID 2272 che il processo "firefox.exe" con PID 3384 utilizzano il file scaricato. Questa attività potrebbe indicare l'utilizzo di un file dannoso o compromesso.
Manual execution by a user: Il processo "powershell.exe" con PID 2272 è stato eseguito manualmente da un utente. Questa attività richiede un'ulteriore indagine per determinare l'intenzione e l'autorizzazione dell'utente.

**Soluzione proposta per la response a un'eventuale infezione da malware:**






L'applicazione Web è stata infettata da un malware e l'obiettivo principale è impedire la propagazione del malware nella rete interna e al contempo evitare la divulgazione di informazioni sensibili verso Internet. La soluzione proposta per affrontare questa situazione comprende le seguenti azioni:

Isolamento dell'applicazione infetta: Isolare l'applicazione infetta creando una rete o un'area separata in cui l'applicazione può operare in modo controllato, impedendo così la propagazione del malware ad altri sistemi o reti.

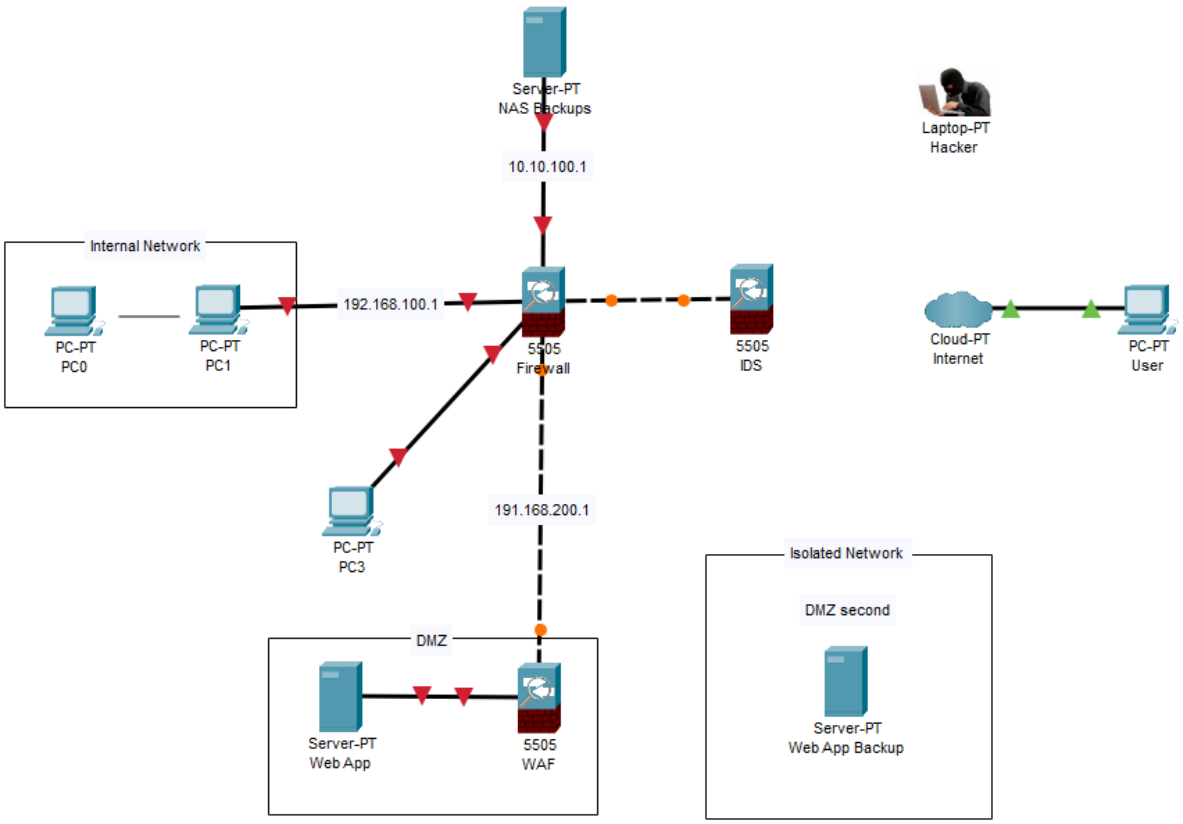
Implementazione di meccanismi di rilevamento e monitoraggio: Installare soluzioni di sicurezza avanzate per il rilevamento e il monitoraggio delle attività sospette all'interno dell'applicazione e del sistema.

Questo permette di identificare tempestivamente eventuali tentativi di propagazione del malware o attività anomale.

Pulizia e ripristino dell'applicazione: Rimuovere il malware dall'applicazione infetta utilizzando soluzioni antivirus e antimalware aggiornate. In seguito, ripristinare l'applicazione a uno stato di sicurezza verificato, riparando o sostituendo eventuali componenti compromessi.
Revisione delle politiche di sicurezza: Rivedere le politiche di sicurezza dell'organizzazione per garantire che siano adeguatamente configurate e che comprendano misure aggiuntive per prevenire futuri attacchi di malware.
Formazione e consapevolezza degli utenti: Condurre programmi di formazione per gli

utenti dell'applicazione, sensibilizzandoli riguardo alle pratiche di sicurezza informatica e ai potenziali rischi. In questo modo, gli utenti saranno in grado di riconoscere e segnalare comportamenti sospetti o attività anomale.

**Conclusioni:**




L'analisi della sicurezza dell'applicazione Web ha evidenziato l'implementazione di azioni preventive efficaci per mitigare i rischi di attacchi SQLi e XSS. Tuttavia, sono state riscontrate attività sospette in due link forniti, che richiedono ulteriori indagini e azioni correttive per garantire la sicurezza dell'applicazione. In caso di un'eventuale infezione da malware, sono state proposte soluzioni di response per limitare la propagazione del malware, ripulire l'applicazione infetta e rafforzare le politiche di sicurezza.

È fondamentale che l'organizzazione mantenga una vigilanza costante sulla sicurezza dell'applicazione Web e adotti misure proattive per proteggerla da potenziali minacce. Inoltre, è consigliabile effettuare regolarmente test di penetrazione e aggiornare le politiche di sicurezza in base all'evoluzione delle minacce informatiche.