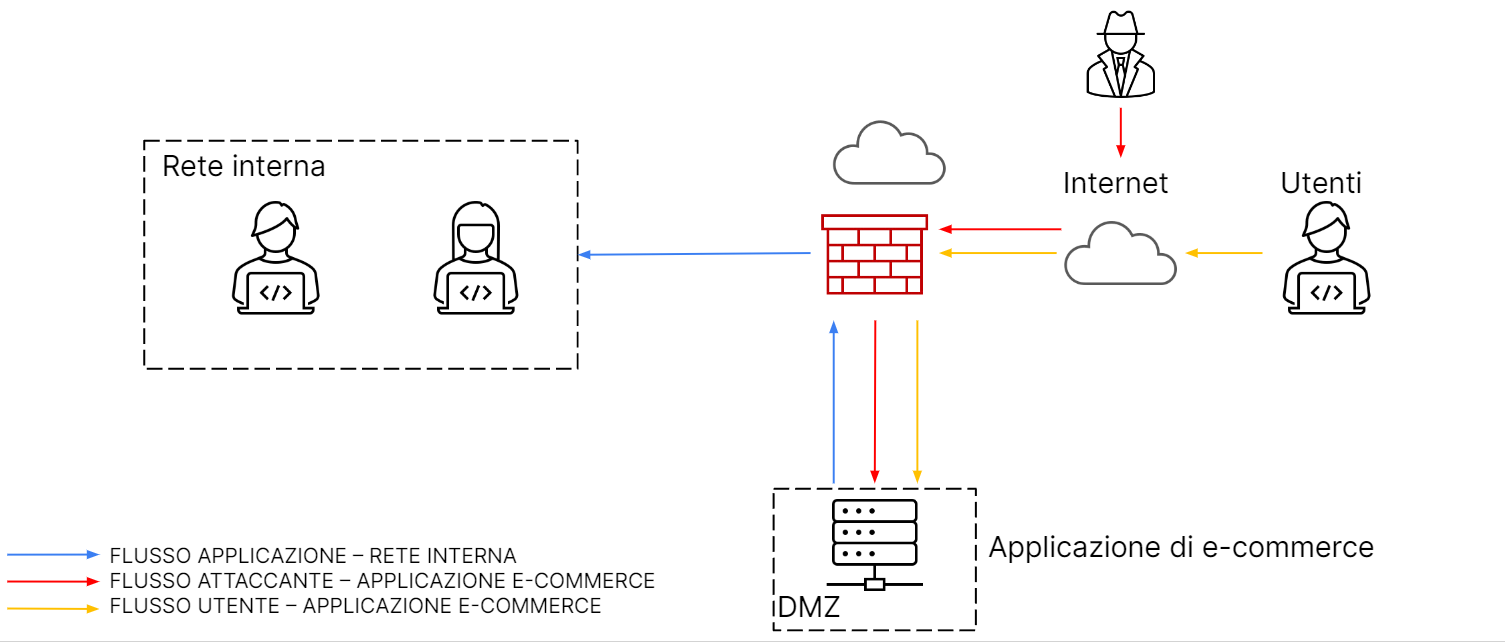
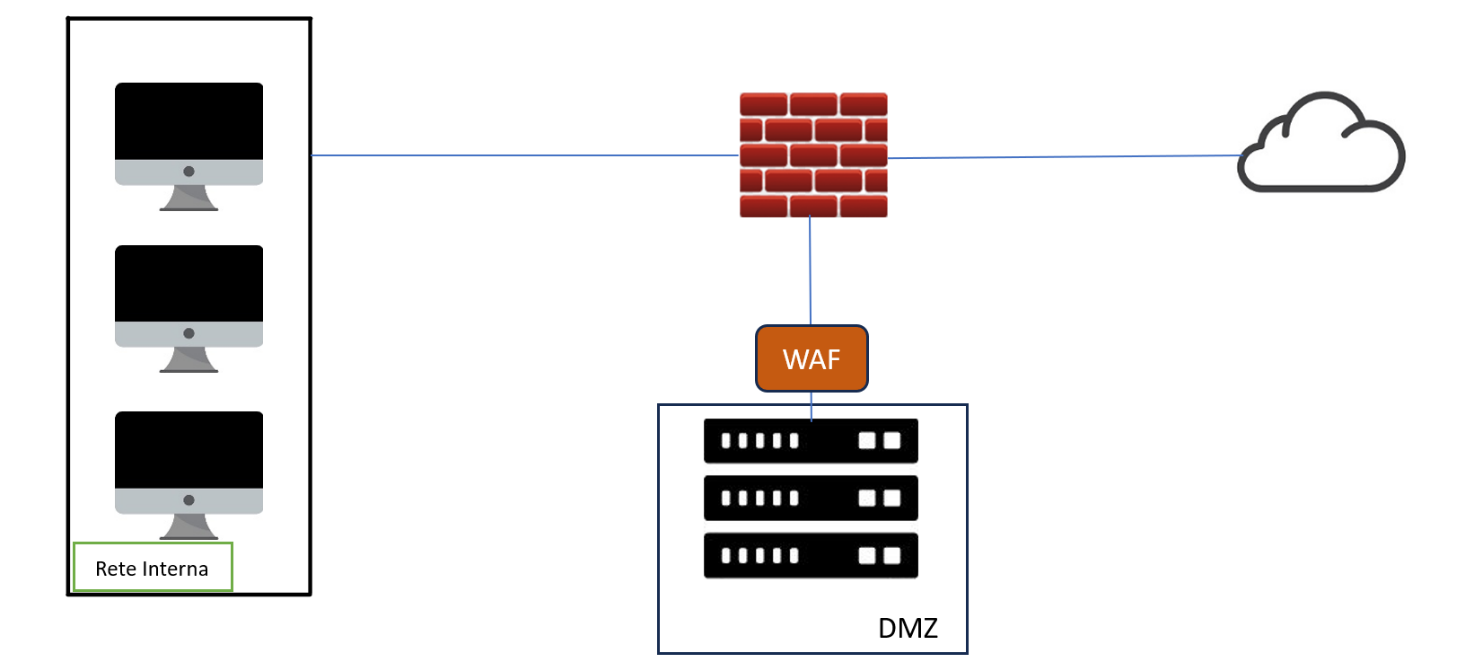
Pierluigi Amorese

Progetto Giorno 5

La traccia di oggi ci propone di attuare delle azioni preventive, di analisi e di response di un caso reale.

Data la figura sottostante il primo punto della traccia ci chiede quali azioni preventive si possono effettuare per difendere l’applicazione web da attacchi di tipo SQLi e XXS.

Come soluzione si propone di aggiungere come sistema di sicurezza un Web Application Firewall (WAF) ovvero un firewall che monitora, filtra e blocca i pacchetti di dati mentre viaggiano da e verso un sito Web o un'applicazione Web.

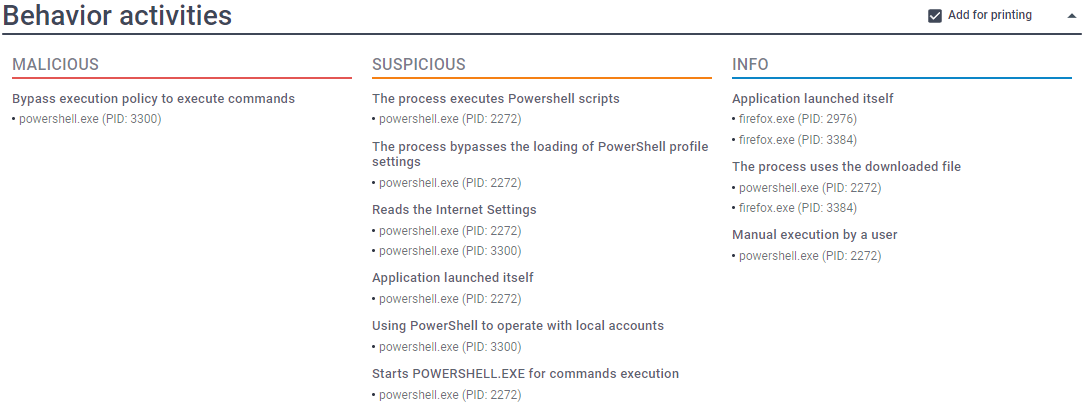


Come secondo task, la traccia ci chiede di analizzare i seguenti siti: <https://tinyurl.com/linklosco1> <https://tinyurl.com/linklosco2>

Immagine che contiene testo, software, schermata, Software multimediale

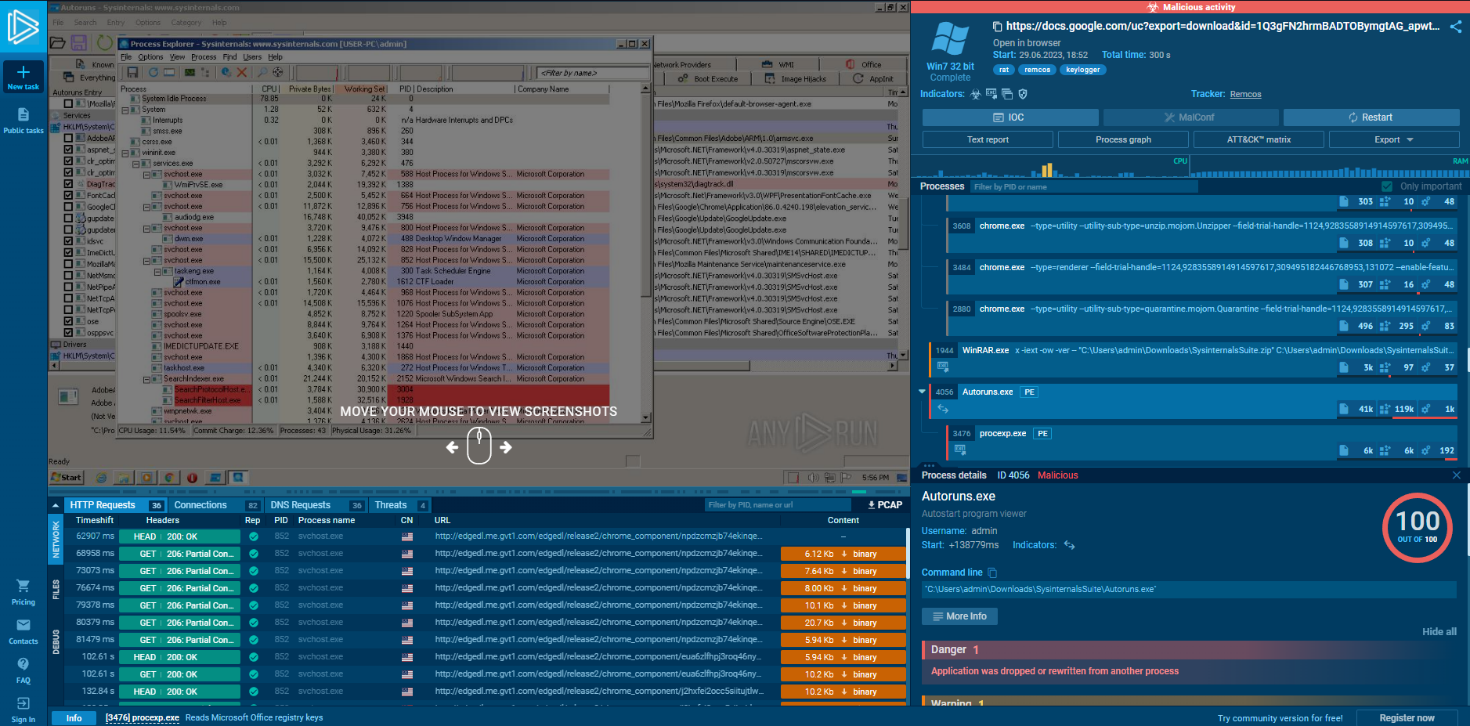
Descrizione generata automaticamente

Aprendo il primo link veniamo reindirizzati verso una pagina di Any.run e tramite il report possiamo capire di cosa si tratta:

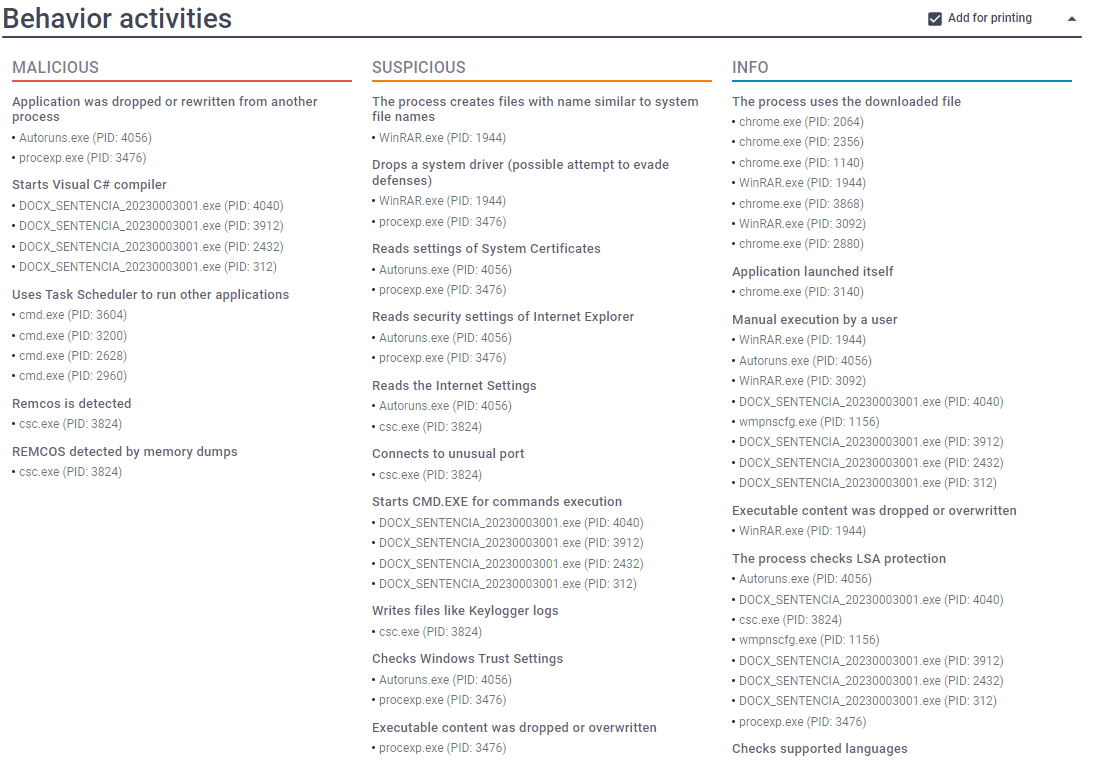


L’analisi ci permette di capire che si tratta di uno script in grado di aprire (grazie a permessi da amministratore di default) in automatico una shell sulla macchina vittima.

Nel secondo link viene analizzato Remcos Rat o Remote Control and Surveillance, commercializzato come un software legittimo per gestire in remoto i sistemi Windows.



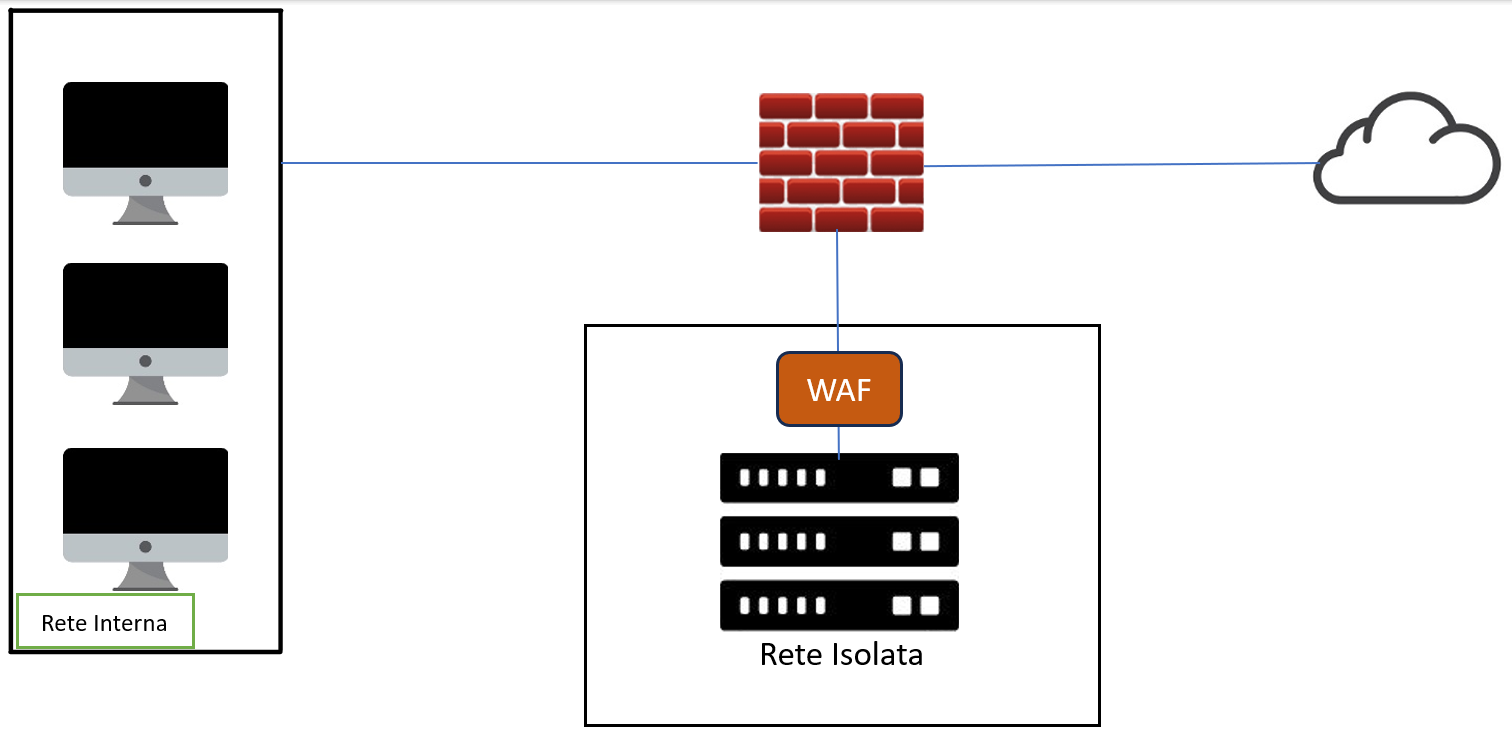
Remcos è un sofisticato Trojan di accesso remoto (RAT) che può essere utilizzato per controllare e monitorare completamente qualsiasi computer Windows da XP.



Nonostante il programma abbia intenzioni legittime, si capisce perché sia utilizzato in maniera malevola, infatti esso permette all’attaccante di controllare il computer infetto da remoto; si possono eseguire comandi, accedere ai file, monitorare le attività dell'utente, registrare la tastiera e la webcam, e persino rubare informazioni sensibili. Se ciò non dovesse bastare, RAT ha la capacità di mantenere la sua presenza nel sistema infetto, in modo da poter essere riattivato in futuro anche dopo un riavvio del computer.

Nella terza parte dell’esercitazione la traccia ci dice che l’app web è stata infettata da un malware. Il nostro compito sarà quello di evitare la propagazione di esso sulla rete interna e impedire la divulgazione delle informazioni sensibili verso internet.

Immagine che contiene design

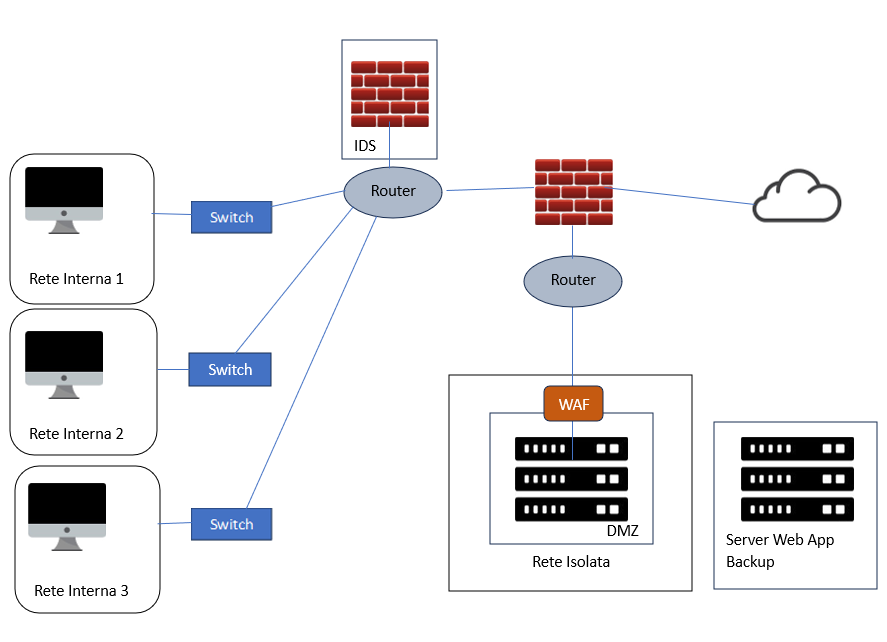
Descrizione generata automaticamente



Server Web App Backup

In questa parte dell’esercizio troviamo l’app web in Isolamento ed il backup già pronto all’uso.

La quarta ed ultima parte dell’esercizio richiedeva di unire le configurazioni di rete del primo e del terzo punto.



Quindi nel complesso le azioni che sono state eseguite per migliorare il livello della rete sono:

* Inserito WAF per avere protezione contro attacchi mirati alle applicazioni web e da possibili vulnerabilità;
* aggiunti switch separati per reti diverse in modo di segmentare la rete limitando la propagazione di minacce;
* aggiunto backup nella rete isolata che permette di separare i dati di backup dalla rete principale;
* aggiunti un router tra il firewall e la rete DMZ e un router tra firewall e rete interna come ulteriore strato di protezione per limitare l’accesso non autorizzato ai sistemi;
* aggiunto IDS collegato al router della rete interna come ulteriore protezione.