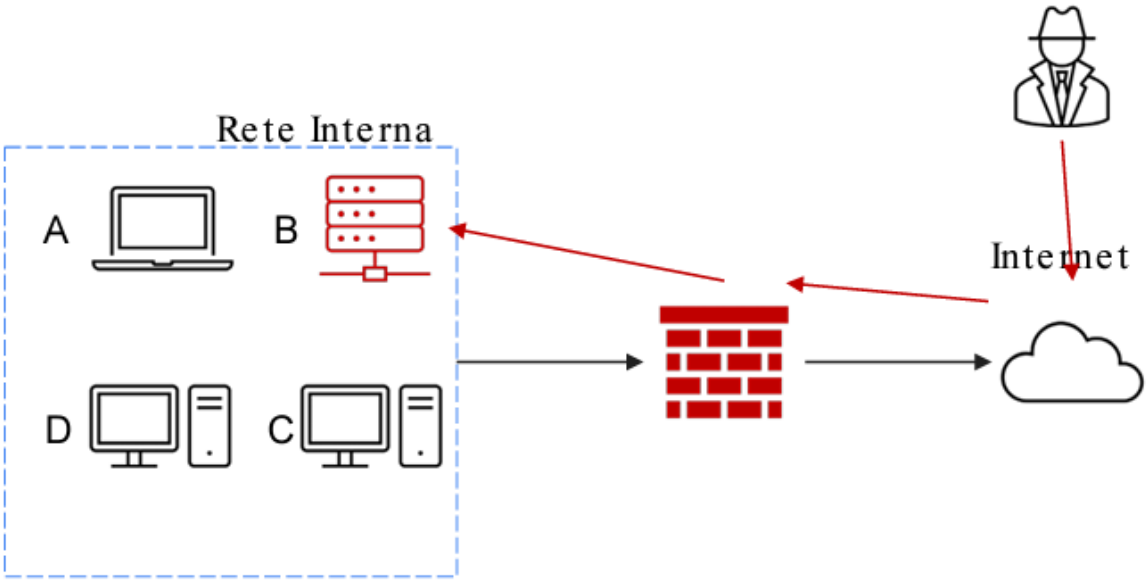
S9L4

Consegna:

La consegna di oggi richiede di agire come se si fosse parte di un CSIRT per fornire informazioni sulle possibili manovre da adottare, in questo caso viene esplicitato che lo scenario dell'esercizio è di un attacco in corso (riportato come immagine).



Inoltre, viene esplicitamente richiesto di:

- Esporre le strategie di Isolamento e Rimozione

- Spiegare la differenza tra Purge e Destroy (nominando anche Clear)

Esecuzione:

Nel contesto fornito dalla consegna è possibile riconoscere un attacco eseguito tramite internet che ha colpito il database (sistema B) di una rete interna, procurando danni ai suoi dischi di memoria e ai dati contenuti in essi.

Normalmente si dovrebbe procedere tramite la tecnica dell'isolamento, che consiste nel disconnettere il dispositivo vittima dalla rete per evitare che infetti gli altri e per rendere più difficile la diffusione dell'attacco, permettendo di guadagnare tempo per poter analizzare meglio l'attacco che sta avvenendo, o per pensare ad altre strategie difensive. Infatti, il dispositivo infetto avrebbe ancora accesso ad internet e per diffondere spargere eventuali malware basterebbe fare un altro attacco. Questa strategia non risulta essere particolarmente risolutiva in questo caso poiché si rimanderebbe il problema.

Nel caso si volesse isolare totalmente un dispositivo infetto durante un attacco si dovrebbe procedere con la tecnica di Rimozione, che non solo prevede la disconnessione del dispositivo dalla rete interna (come nell'isolamento), ma gli impedisce di accedere ad

internet. In questa maniera si impedisce qualsiasi tipo di comunicazione con il dispositivo infetto, rendendola obsoleta e prevenendo qualunque tipo di attacco che possa effettuare la macchina infetta.

Dopo aver messo in quarantena il dispositivo vittima, generalmente si dovrebbero eseguire delle procedure per la sanificazione di tale dispositivo. Quelle che riescono a garantire meglio la rimozione di codici malevoli sono:

- Purge: che consiste nel ripristinare una macchina tramite dei meccanismi (detti fisici) che riescono a mantenere intatta la macchina, ma che la svuota di tutti i dati contenuti (spesso vengono utilizzati dei magneti).

- Destroy: che consiste nello smaltimento della macchina poiché oramai resa obsoleta o perché contenente dati sensibili (solitamente i dispositivi vengono disintegrati)

Un ulteriore metodo utilizzato per la sanificazione di un dispositivo vittima di un attacco è Clear, che si differenzia dai due metodi precedenti perché agisce solo e soltanto tramite metodi processabili dalla macchina infetta senza andare ad interagire fisicamente con qualcosa che non sia il dispositivo in questione, a differenza del Purge che prevede l'utilizzo di meccanismi esterni, oppure del Destroy che disintegra le macchine sanificate.