Epicode
CS-0124
Pratica S9/L4

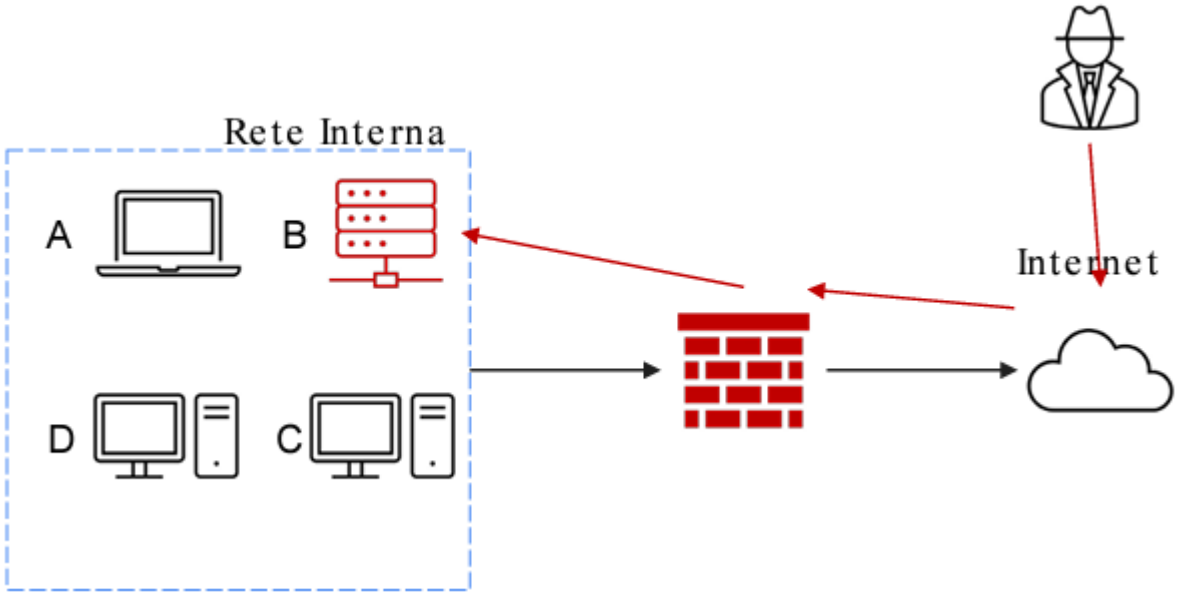
Francesco Ficetti

Traccia

Con riferimento alla figura seguente, il server B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante, che è riuscito a bucare la rete ed accedere al sistema tramite Internet.

Rispondere ai seguenti quesiti.

- Mostrare le tecniche di isolamento e rimozione del sistema infetto.
- Spiegare la differenza tra clear, purge e destroy per l'eliminazione delle informazioni sensibili.



Svolgimento

La tecnica dell’isolamento consiste nella completa disconnessione del sistema infetto dalla rete, per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante. In questo caso, il server B sarebbe collegato in modo tale che avrebbe ancora accesso ad internet, ma non al resto della rete interna.
La tecnica della rimozione è la più estrema consiste nella completa rimozione del sistema sia dalla rete sia interna che esterna.

Durante la fase di recupero, ci si trova spesso a dover gestire lo smaltimento o il riutilizzo di un disco o un sistema di storage. In questo caso, bisogna accertarsi in prima istanza che le informazioni presenti sul disco/componente siano completamente inaccessibili prima di smaltire/utilizzare nuovamente il disco.
Si possono individuare tre opzioni per la gestione dei media contenenti informazioni sensibili:

- Clear: il dispositivo viene completamente ripulito dal suo contenuto con tecniche logiche. Si utilizza, ad esempio, un approccio di tipo *read and write* dove il contenuto viene sovrascritto più e più volte o si utilizza la funzione di *factory reset* per riportare il dispositivo nello stato iniziale.
- Purge: si adotta non solo un approccio logico per la rimozione dei contenuti sensibili, ma anche tecniche di rimozione fisica come l’utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi.
- Destroy: è l’approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili. Oltre ai meccanismi logici e fisici, si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione ad alte temperature o trapanazione. Questo metodo è sicuramente il più efficace per rendere le informazioni inaccessibili ma è anche quello che comporta una spesa maggiore.