REPORT 22/12/2022

FACCILONGO DOMENICO

INCIDENT RESPONSE

TASK

Con riferimento alla figura in slide 4, il sistema **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.

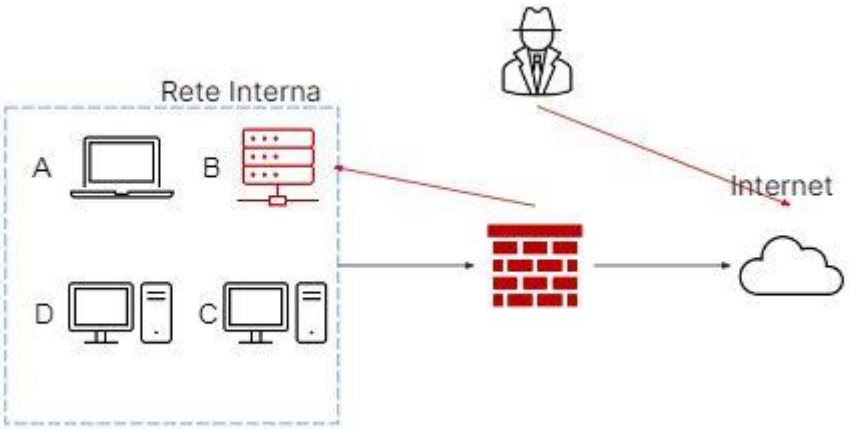
L'attacco è attualmente in corso e siete parte del team di CSIRT.

Rispondere ai seguenti quesiti.

- Mostrate le tecniche di: I) **Isolamento** II) **Rimozione** del sistema **B infetto**
- Spiegate la differenza tra **Purge** e **Destroy** per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. **Indicare anche Clear**

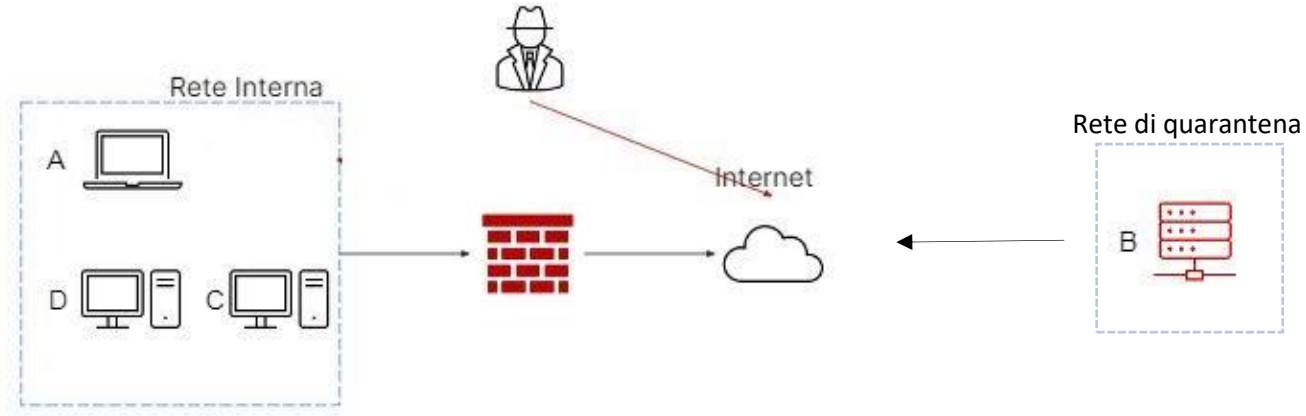
RISOLUZIONE DEL PROBLEMA

Sulla base della figura di cui di seguito andare a risolvere il problema che segue: **Isolare** e **Rimuovere** il sistema B infetto.



- **ISOLAMENTO**

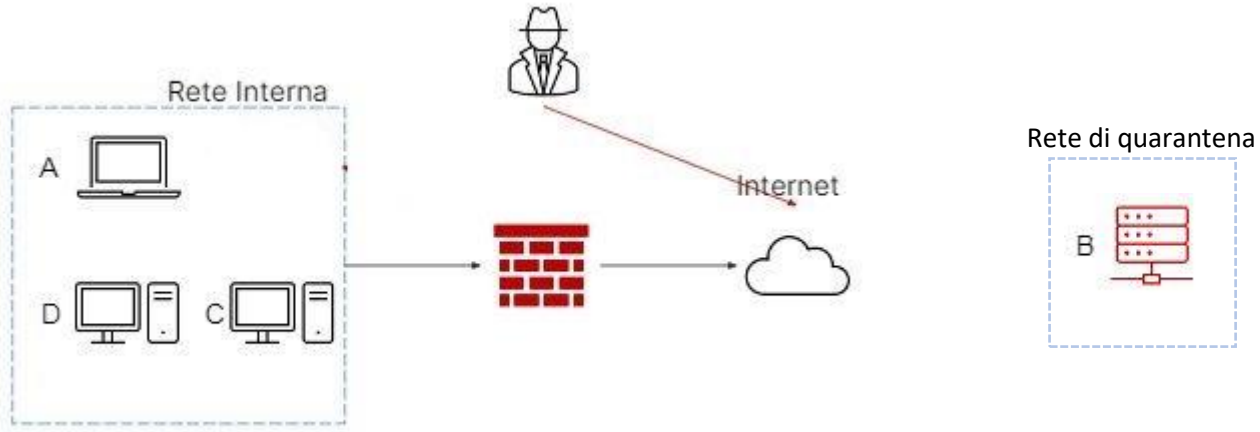
Come primo approccio prendiamo in esame di voler isolare il database infetto (B). Partendo dal presupposto che il Database può infettare gli altri dispositivi collegati sulla stessa rete. Per prima cosa dobbiamo considerare che il Database fa parte di una rete interna, pertanto, dobbiamo creargli una rete propria interna distaccandola da quella iniziale. Così facendo l'attaccante può ancora controllare il Database in quanto collegato via Internet. Il risultato è pressocchè questo:



Così facendo abbiamo il database appartenente ad un'altra rete interna chiamata **rete di quarantena** e l'attaccante non potrà più infettare altri dispositivi, i quali ORA appartengono ad un'altra rete interna (ovvero quella iniziale). A questo punto possiamo approfittare per sniffare l'attaccante e ottenere il suo IP in modo tale da porlo in una **black list**.

- **RIMOZIONE**

In tal caso invece andiamo a rimuovere il database infetto dalla rete interna e anche dalla possibilità di comunicare con Internet.



Il risultato è che l'attaccante non avrà più possibilità di accesso al nostro database.

ELIMINAZIONE DELLE INFORMAZIONI SENSIBILI

Avendo il nostro Database infetto le soluzioni che dobbiamo andare ad applicare sono pressoché tre, ovvero:

1. **CLEAR:** il dispositivo in questione viene completamente ripulito da suo contenuto con tecniche <<logiche>>. Si utilizza per esempio un approccio di sovrascrittura multipla con un massimo di 7 volte per tentare il recupero dei dati persi, o si utilizza la funzione di <<factory reset>> ovvero riportare il dispositivo allo stato di fabbrica.
2. **PURGE:** In tale caso bisognerà andare a rimuovere forzatamente la componente fisica con l'utilizzo di magneti per rendere le informazioni inaccessibili su determinati dispositivi. Il tutto attraverso l'utilizzo del **DEGAUSSER** un componente che elimina la carica magnetica di un oggetto**.**
3. **DESTROY:** come dice la parola stessa và a distruggere il dispositivo con tecniche di disintegrazione, polverizzazione dei media ed alte temperature. Questo è sicuramente il metodo più efficace tra i tre in quanto rende le informazioni inaccessibili ma è anche quello che comporta però un effort in termini economici maggiori.