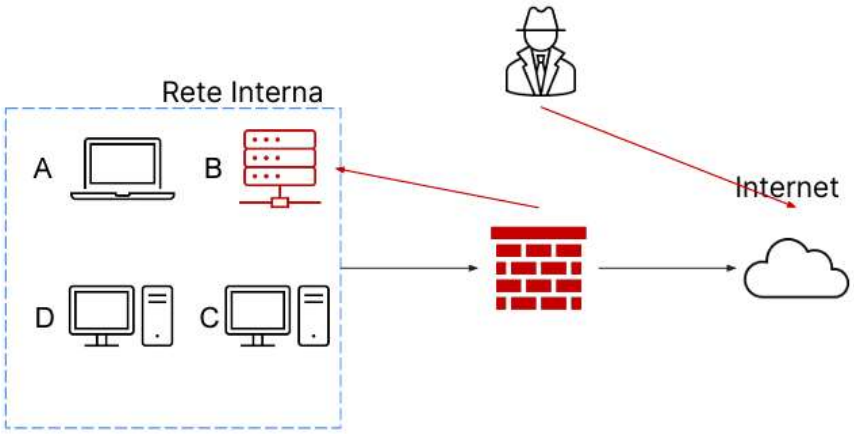
Progetto W9/L4-Incident response

Con riferimento alla figura sotto, 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.

-Mostrare le tecniche di: I) Isolamento II) Rimozione del sistema B infetto

-Spiegare la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi.



Per evitare che l'attaccante, dopo essere entrato sul database B, passi agli altri host possiamo utilizzare come prima tecnica l'isolamento.

Ciò consiste nell'isolare dalla rete interna il database, consiste nella completa disconnessione del sistema infetto dalla rete interna, per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante. In questo caso però il database infettato è ancora connesso alla rete internet anche se non fa più parte della rete interna. Questo isolamento si può fare attraverso la creazione di una rete VLAN ad hoc per B o una segmentazione della rete attraverso una subnet dedicata.

Il passo successivo può essere quello di rimuovere dalla rete il sistema B infetto, per fare ciò basterebbe scollegarlo dalla rete fisicamente così che l'attaccante non riesca più a comunicare con l'host infetto dato che non ha più connessione ad internet.

Per l'eliminazione delle informazioni sensibili dagli hard-disk infetti possiamo usare

tre metodi: -Clear -Purge -Destroy

Andiamo ad analizzare Purge e Destroy:

-Purge: con questo sistema si adotta non solo un approccio logico per la rimozione dei contenuti sensibili, come visto nel caso di clear, 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 appena visti, si utilizzano tecniche più drastiche come la frammentazione fisica dell'hardware, esempio forandolo in vari punti o polverizzandolo. Sicuramente questa tecnica è la più sicura per evitare il recupero di informazioni sensibili da parte di terzi, ma è anche la più drastica e dispendiosa.