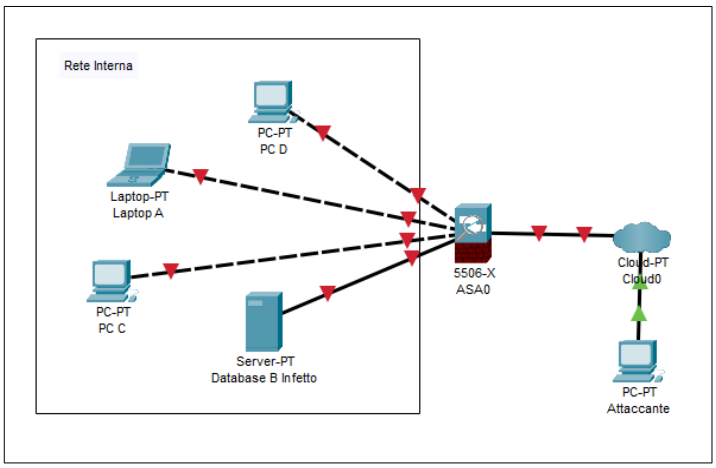
Incident Response

Obiettivo: Mostrare le tecniche di Isolamento e Rimozione di un Database compromesso e mostrare le tecniche di pulizia e recupero dati.

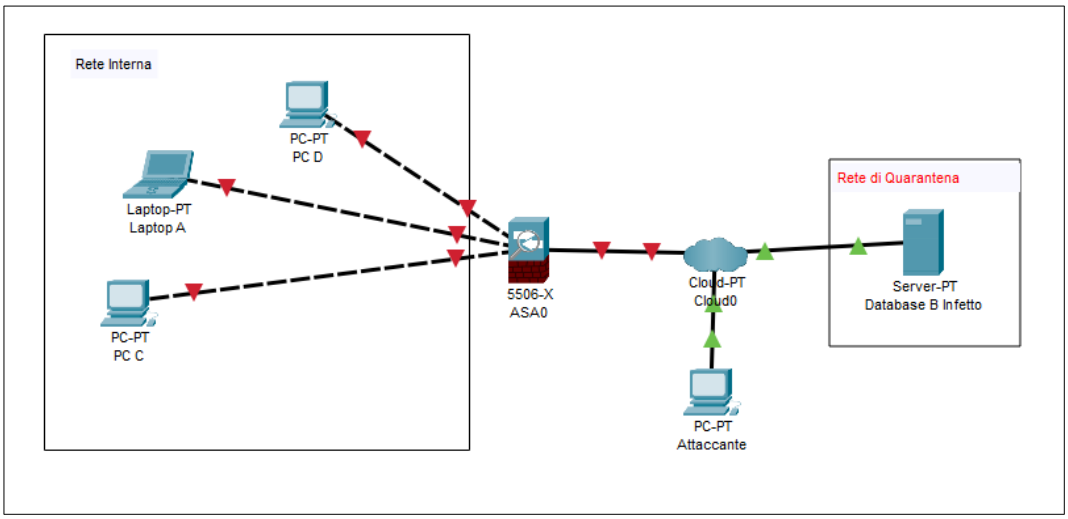
1) Situazione Attuale

La situazione che ci viene posta è la seguente: il **Database B** è stato compromesso da un attaccante che è riuscito ad entrare nella rete interna tramite **Internet**. La traccia ci chiede di mostrare le tecniche di ***Isolamento*** e di ***Rimozione*** per escludere il **Database** colpito dalla **Rete Interna** ed evitare che altri apparecchi vengano colpiti.



2) Isolamento

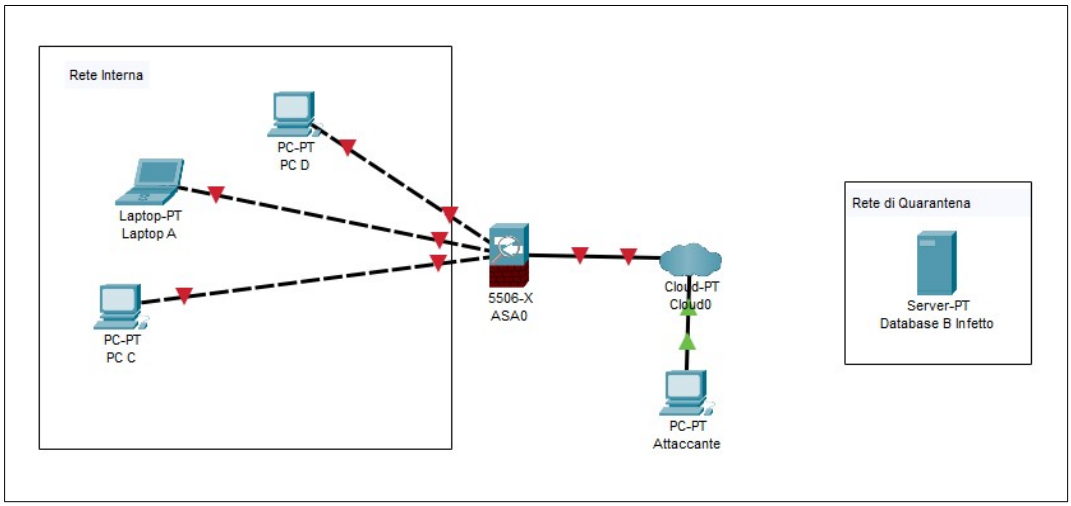
Si procede col disconnettere il **Database** colpito dall'hacker dalla **Rete Interna**, in maniera tale che l'attaccante abbia un campo d'azione ristretto e non possa quindi colpire altri *Client*.



Si stabilisce perciò una **Rete di Quarantena** che permette comunque all'attaccante di restare connesso al **Database** ma allo stesso tempo permette al *Team CSIRT* di contenere il danno causato dall'attaccante ed impedire che vengano riprodotti **Malware** o simili su altri nodi.
Questo permette di poter studiare l'attacco e l'attaccante andando ad esempio a leggere i **Log di Sistema** (possono dirci ad esempio l'indirizzo IP sorgente) o **Monitorare il traffico dei Dati** (per vedere gli indirizzi IP che potrebbero essere collegati all'attacco).

3) Rimozione

In alcuni casi il solo Isolamento non è abbastanza, perciò si procede con la Rimozione, ovvero come dice il nome ***Rimuovere*** il **Database** infetto sia dalla **Rete Interna** che da **Internet**.



La ***Rimozione*** è utile oltre al non permettere, ovviamente, l'espandersi dell'attacco ad altri apparecchi, anche al concentrarsi sull'indagine dell'attacco e sulle attività di mitigazione. Possiamo infatti analizzare con calma il **Database** compromesso e nel caso sia presente un *Backup*, rimuovere il **Database**, spostarlo su un Sistema sicuro e recuperare i dati senza il rischio di espandere ad esempio un **Malware** o un **Codice Malevolo**.

4) Clear, Purge e Destroy

- ***Clear*** ha come obiettivo di ripulire il Sistema compromesso dalle tracce dell'attacco in maniera logica ripristinandolo. Si rimuovono i file Dannosi, si patchano le vulnerabilità colpite riportando il Sistema (in questo caso il Database) alle condizioni pre-attacco.

- ***Purge*** elimina definitivamente i Dati sensibili o compromessi che ad esempio sono risultati esposti durante l'attacco. Questo tipo di azione prevede anche la rimozione (o distruzione) fisica dei componenti del Sistema colpito. Questo impedisce il recupero di tali Dati.

- ***Destroy*** è invece la soluzione "drastica", cioè si utilizzano tecniche "estreme" per distruggere completamente i supporti colpiti dall'attacco (come disintegrazione e polverizzazione dei media ad alte temperature). Questa scelta è optata quando non è più possibile recuperare i Dati compromessi in maniera sicura. Si usa come ultima risorsa.