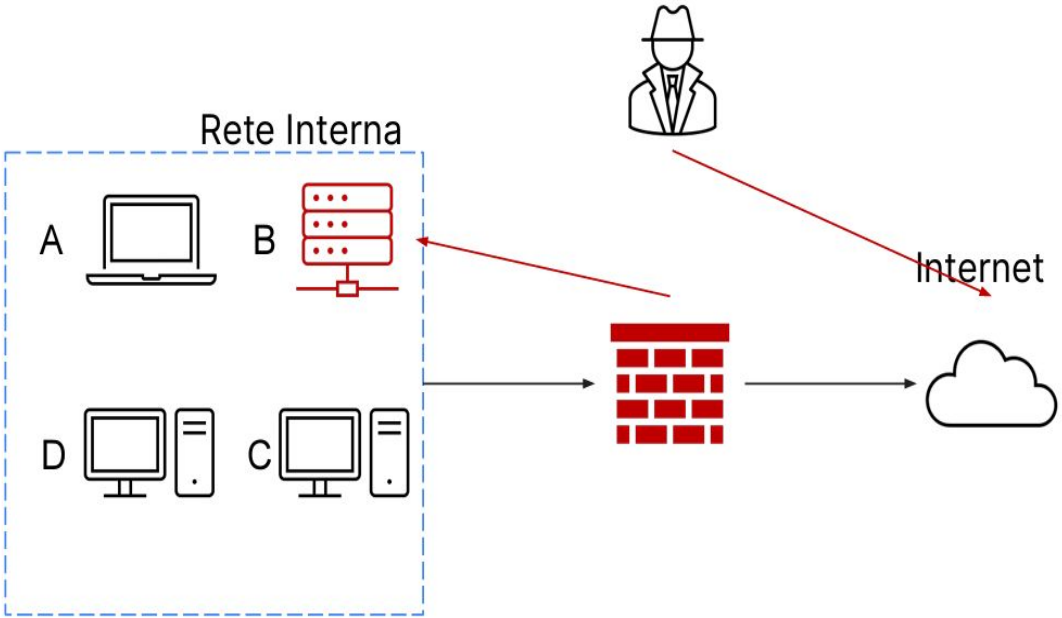
Consegna S9-L4

incident respons



L’esercizio richiede di specificare le eventuali azioni che si possono prendere in caso di attacco come possiamo vedere in figura, attacco ancora in atto per lo piu’

La prima cosa e’ quella di cambiare le regole firewall cosi’ da eliminare la comunicazione tra l'attaccante ed il target, fatto cio’ dobbiamo assicurarci di isolare il sistema B così da poter accertarci che non infetti altri sistemi e che sia ancora correttamente funzionante nel caso lo fosse allora possiamo integrarlo nella nostra rete, ovviamente dopo aver preso le giuste precauzioni. Nel caso invece in cui il sistema sia compromesso si puo’ tentare di resettarlo ma se cio’ non dovesse servire allora bisognera’ eseguire un Clear e installare un backup precedente all’attacco

Purge e Destroy

Purge: con questo termine si fa riferimento al fatto di agire con programmi o funzioni sul disco fisico del sistema lasciando quindi il disco integro.

Destroy: questo termine si riferisce all’azione di polverizzare fisicamente il disco quindi agendo a livello fisico su di esso come per esempio perforarlo con un trapano