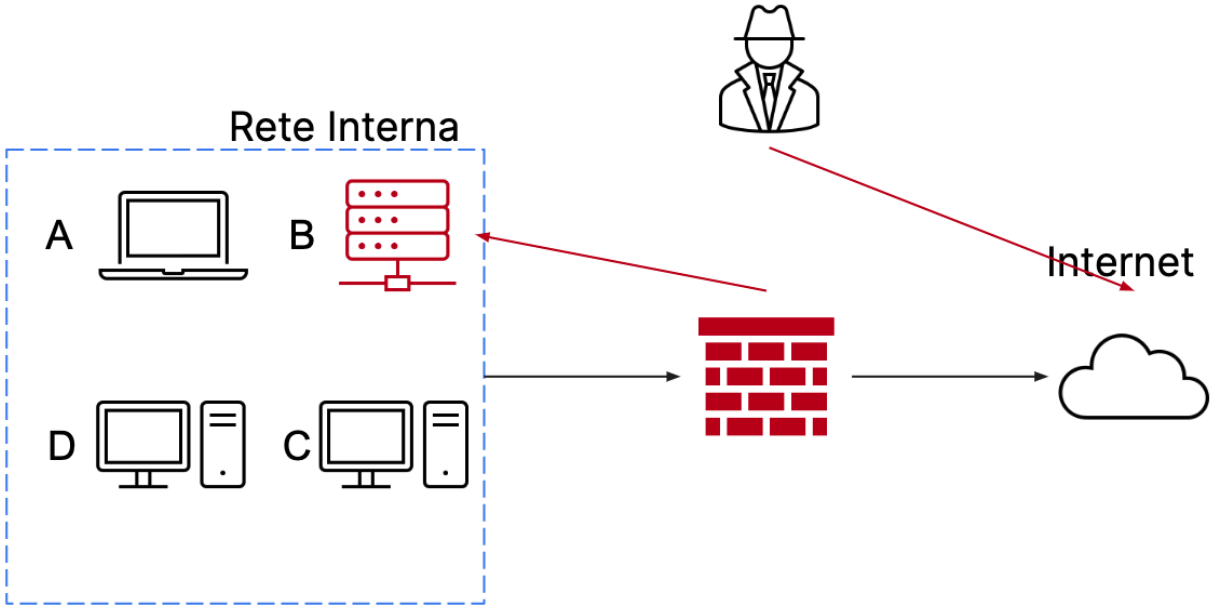
REPORT INCIDENT RESPONSE

FRANCESCO PERSICHETTI

Avendo una situazione come quella in figura, dove un attaccante è riuscito a bucare la rete e ad accedere tramite internet al nostro sistema B

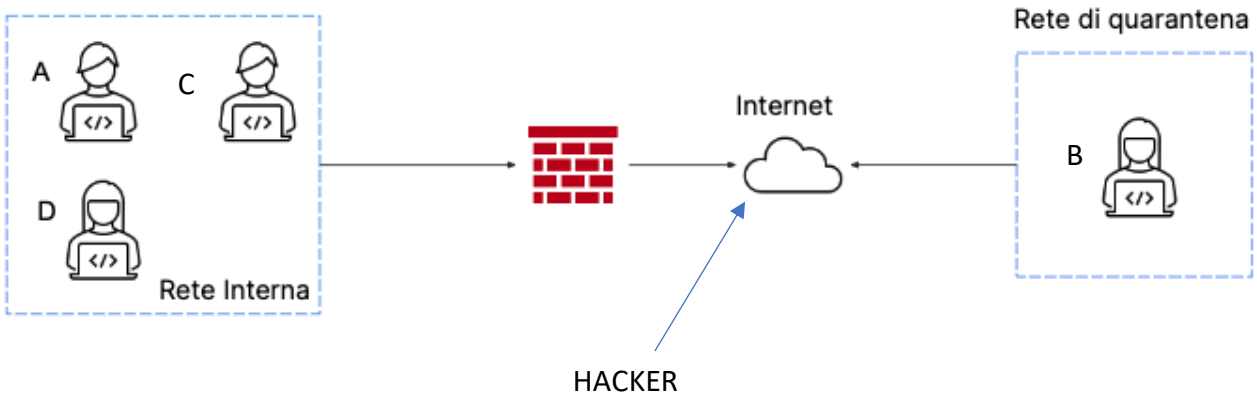


Spiegare i task del giorno:

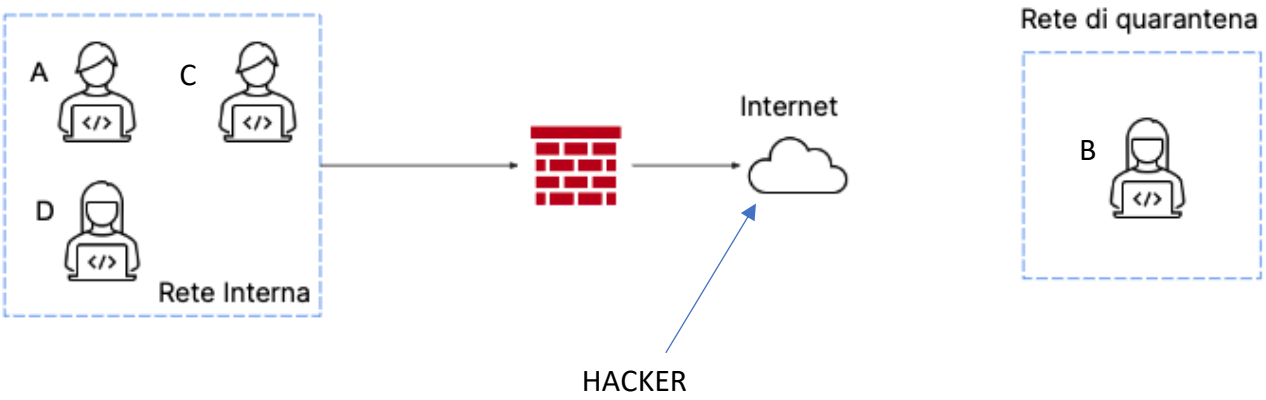
- Tecniche di isolamento e rimozione del sistema B infetto
- Spiegare la differenza tra **Purge**, **Destroy e Clear**

1.

Per assicurarsi che l'attaccante una volta infettato B non possa espandersi andando ad infettare anche gli altri sistemi presenti all'interno della rete Interna a cui fa parte anche B; esistono delle tecniche per cercare di contenere l'attacco verso tutta la rete. Una tra queste è la tecnica **dell'isolamento** che consiste nella completa disconnessione del sistema infetto dalla rete interna per passare ad una rete di quarantena per scongiurare ulteriormente un danno maggiore su tutta la rete, lasciando comunque il sistema B connesso a internet e quindi ancora sotto il possibile controllo dell'attaccante.



L’altra tecnica più stringente dal punto di vista della sicurezza è la completa **Rimozione** del sistema infetto sia dalla rete internet che da quella interna, così da assicurarsi che l’attaccante non possa in nessun modo né avere accesso alla macchina infetta messa nella rete di quarantena né tantomeno alla rete interna.



2.
Una volta occupatosi della fase di contenimento si passa alla fase di recupero dei dati e delle informazioni perse durante l’attacco. Durante questa fase prima dello smaltimento o del riutilizzo di un disco appartenente ad un sistema compromesso, bisogna accertarsi che le informazioni contenute al loro interno siano completamente inaccessibili.
Esistono 3 diverse opzioni:

- **Clear**: dove il disco viene ripulito interamente con tecniche “logiche”. Si cerca di sovrascrivere i dati più e più volte o con processi di “reset” fino a riportare il dispositivo allo stato iniziale.

- **Purge**: oltre a adottare tecniche “logiche” come nel caso del Clear, si usano anche tecniche più “fisiche” come l’utilizzo di forti magneti per rendere impossibile l’accesso alle informazioni anche da parte di determinati dispositivi.

- **Destroy**: a differenza delle due opzioni precedenti e in aggiunta alle tecniche viste fin ora, in questo caso si utilizzano anche tecniche di “laboratorio” come disintegrazione e polverizzazione dei media ad alta temperatura. E’ sicuramente il metodo più efficace ma anche il più dispendioso in termini economici