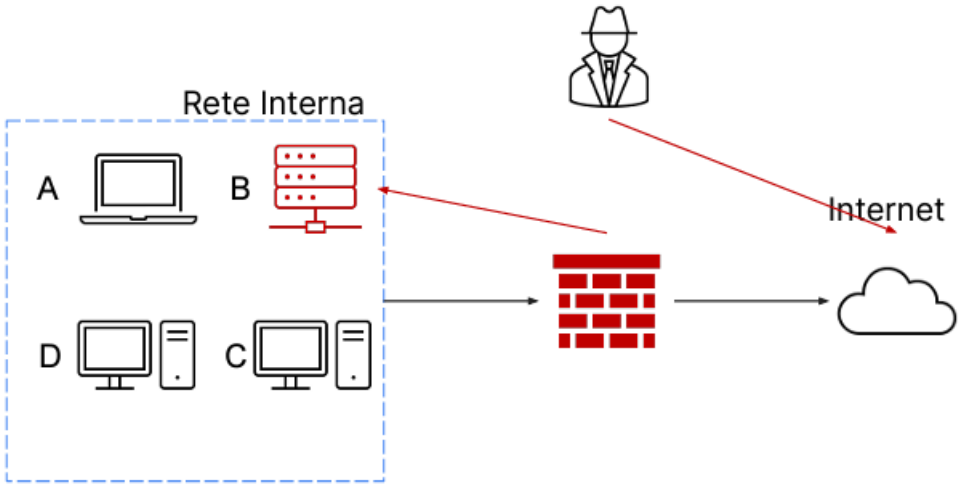
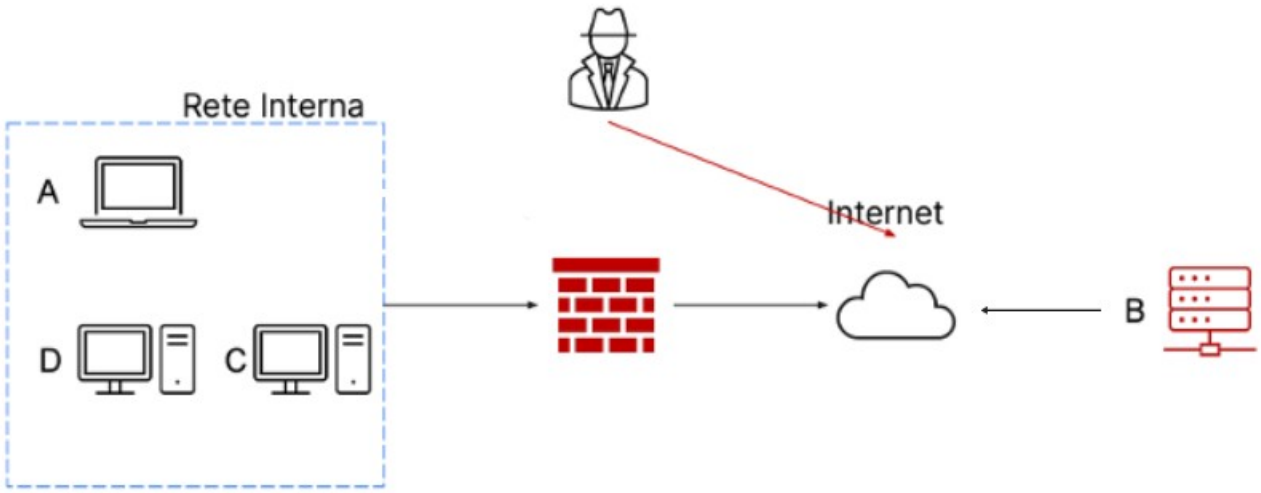
INCIDENT RESPONSE

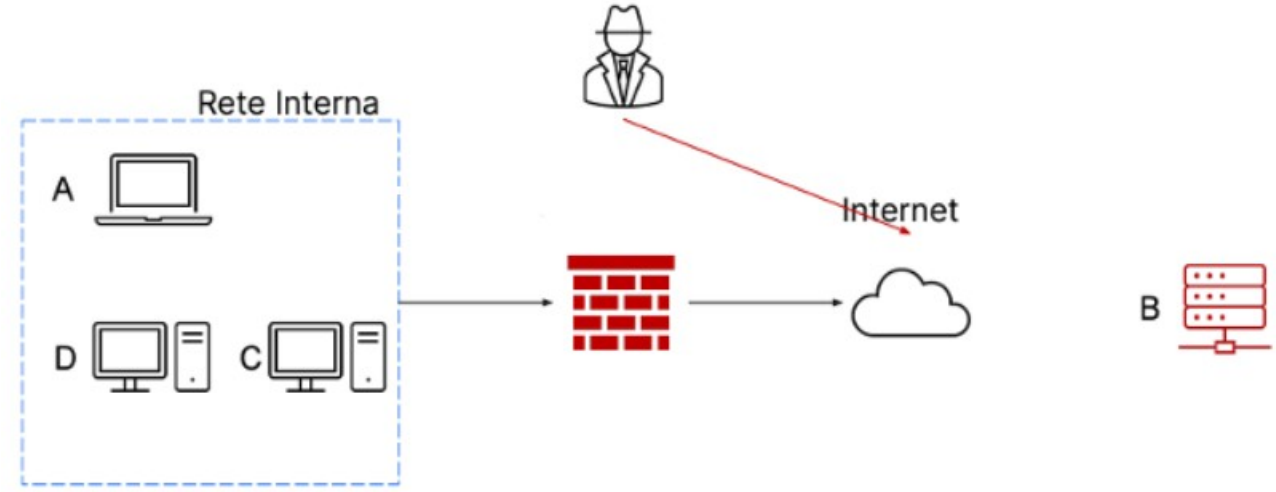
Con riferimento alla figura sotto, il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete e ad accedere al sistema tramite Internet. L'attacco è attualmente in corso e siete parte del team di CSIRT.
Mostrate le tecniche 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.



Per prima cosa è necessario isolare il sistema infetto dal resto della rete, per evitare che l'attaccante possa sfruttarla per penetrare altri dispositivi. L'isolamento consiste nel rimuovere il sistema dall rete in cui si trova e spostarlo su un'altra rete, detta di quarantena, sfruttando la segmentazione. In questo caso il sistema infetto potrà essere raggiunto solo da Internet, ma non avrà alcuna connessione con la LAN dell'azienda.



Se l'isolamento non basta a contenere l'attacco, è possibile ricorrere alla rimozione del sistema, tagliando anche la sua connessione ad Internet e lasciandolo quindi completamente isolato.



Una volta finito l'attacco, bisogna decidere quale azione intraprendere per rimuovere i dati sensibili dal database compromesso prima che i suoi dischi vengano smaltiti. Possiamo ricorrere a diverse azioni, tra cui “Purge” e “Destroy”.

Con Purge si intende un approccio misto, che usa tecniche di rimozione logiche (read and write o factory reset) e fisiche (uso di magneti per smagnetizzare gli hard disk).

Destory è il metodo più drastico, in quanto otlre all'eliminazione dei dati, si va anche a distruggere fisicamente i dischi.

Il metodo scelto dipende dallo stato di compromissione del dispositivo infetto; se si ritiene che esso è ancora utilizzabile ed ogni traccia dell'attacco è stat rimossa, è bene procedere con un metodo che permetta di recuperarlo; se invece esso è definitavemnte compromesso, è meglio procedere anche all distruzione fisica.