

INCIDENT RESPONSE

MATTIA PASTORELLI

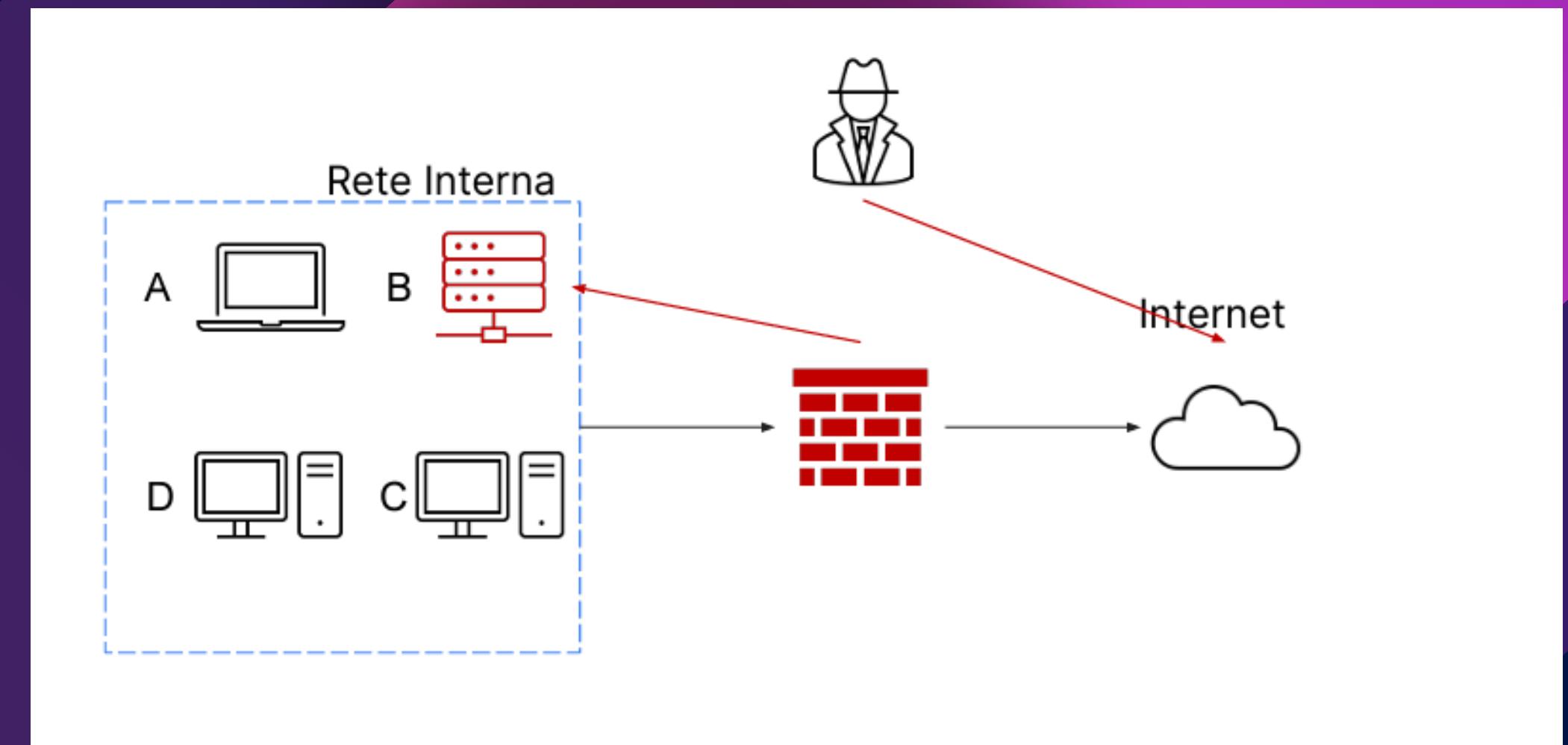


COMANDA:

Con riferimento alla figura in slide 4, 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.

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

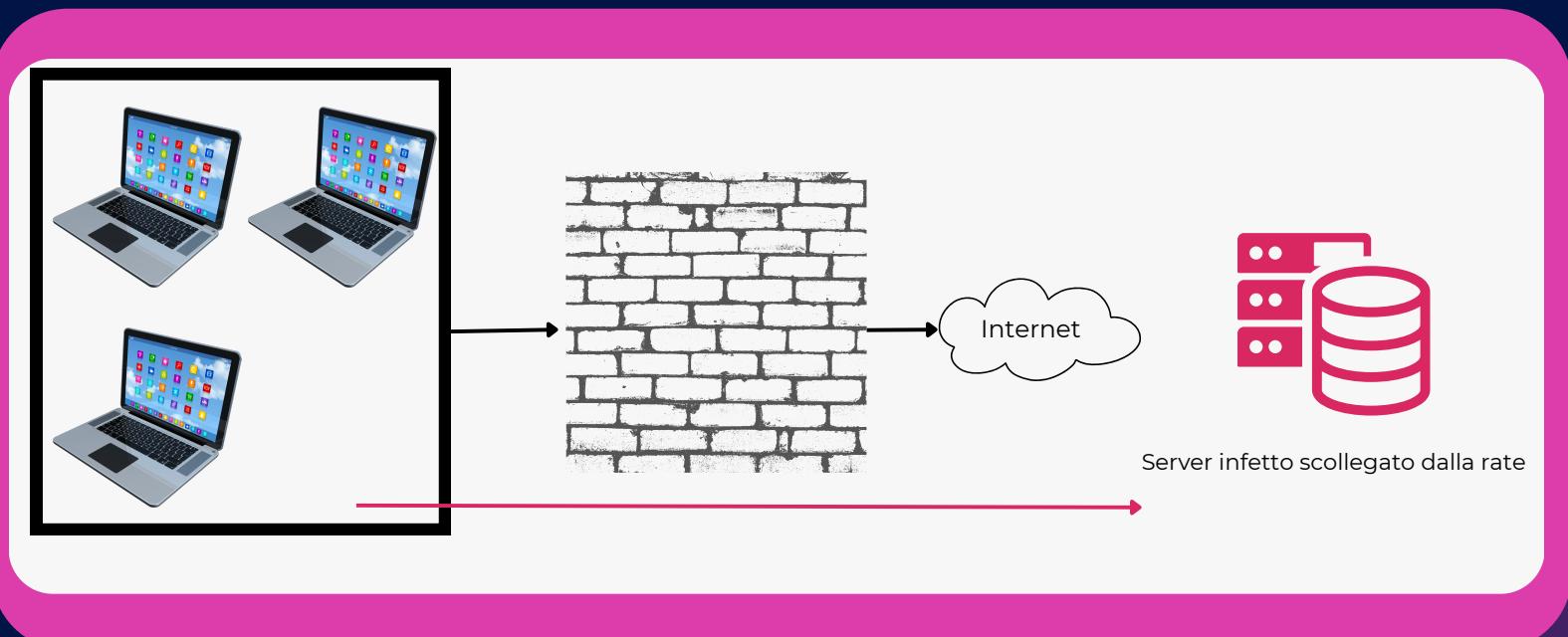
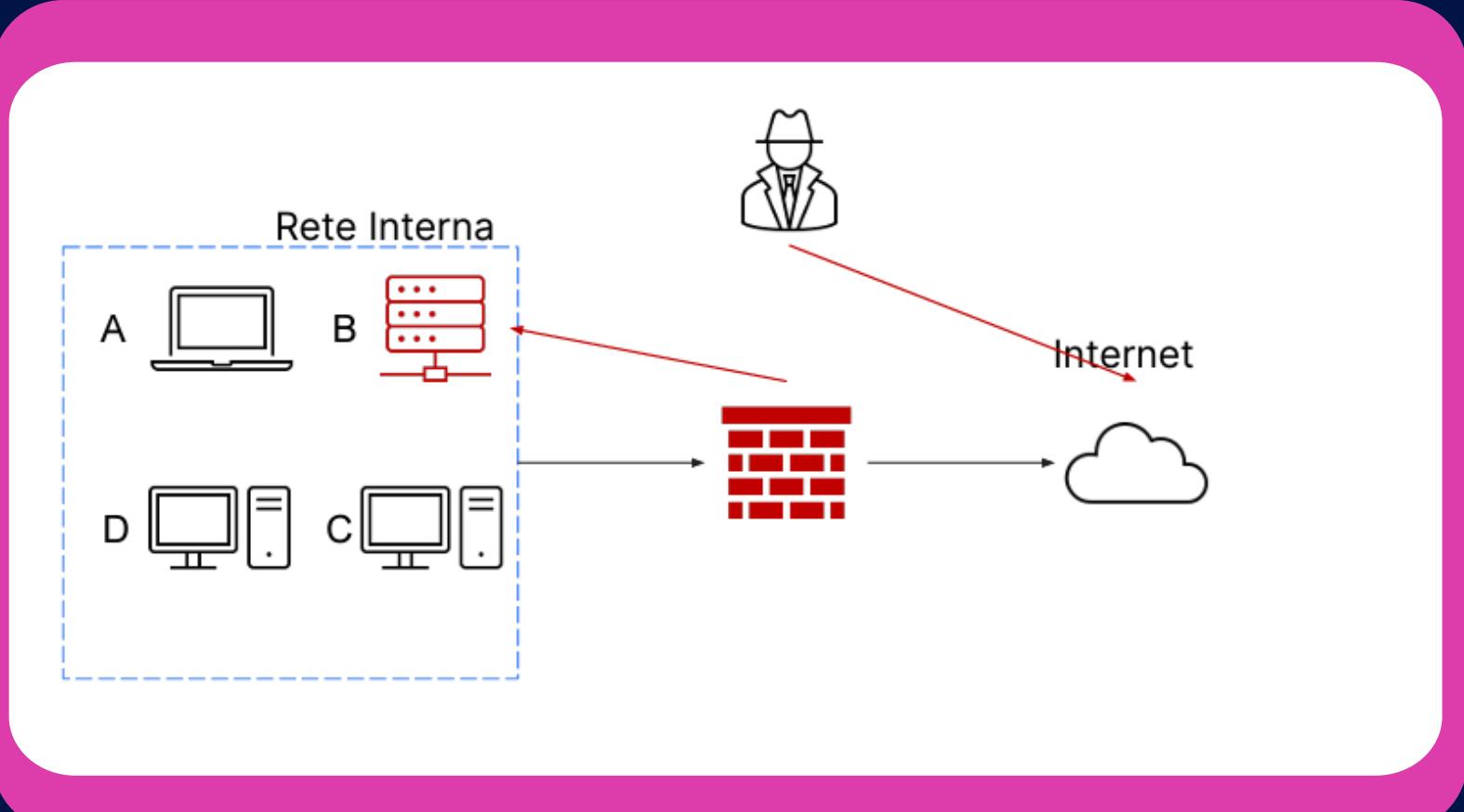
Spiegate la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi



ISOLAMENTO & RIMOZIONE DEL SISTEMA “B” INFETTO:

Ci sono diverse metodologie per isolare un sistema:

- Il primo approccio consiste nella segmentazione di rete tramite VLAN. In questo modo, il dispositivo B viene inserito in una specifica segmentazione di rete chiamata "Rete di quarantena". (Efficace contro un malware, meno contro un hacker)
- Se il primo metodo non è efficace poiché può essere aggirato (pivoting), si può optare per il trasferimento del sistema B al di fuori dell'azienda, ossia in isolamento, su una rete esterna. (L'attaccante avrà comunque accesso alla macchina bersaglio e a Internet)
- Nel caso in cui nemmeno questa strategia funzioni, si può ricorrere alla soluzione più radicale: disconnettere completamente il sistema bersaglio dalla connessione. Questo significa che l'attaccante non potrà più accedere alla macchina bersaglio né a Internet tramite quel sistema.



DIFFERENZA TRA “CLEAR” “PURGE” E “DESTROY”

CLEAR: Il dispositivo viene completamente ripulito dal suo contenuto con tecniche logiche. Si utilizza, per esempio, un approccio read and write, dove il contenuto viene sovrascritto più e più volte, o si utilizza la funzione “Factory Reset” per riportare il dispositivo alle impostazioni di fabbrica.

PURGE: si riferisce generalmente all'azione di eliminare o rimuovere qualcosa, solitamente in modo completo e definitivo. Ad esempio, si potrebbe "purgare" una cache, eliminando tutti i dati memorizzati al suo interno, o "purgare" un database, eliminando tutte le voci in esso contenute.

DESTROY: si riferisce anche all'azione di eliminare qualcosa, ma può avere implicazioni più forti. Mentre "purge" indica spesso una rimozione completa e definitiva, "destroy" può suggerire una distruzione più drastica o irreversibile.

