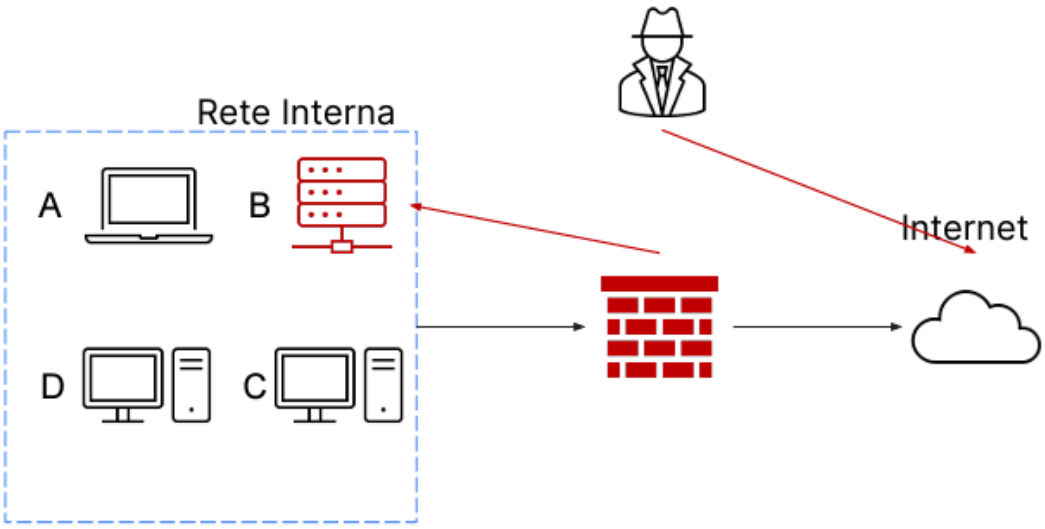
Incident Response

Davide Diglio



Traccia

Il sistema B è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet.

Rispondere ai seguenti quesiti:

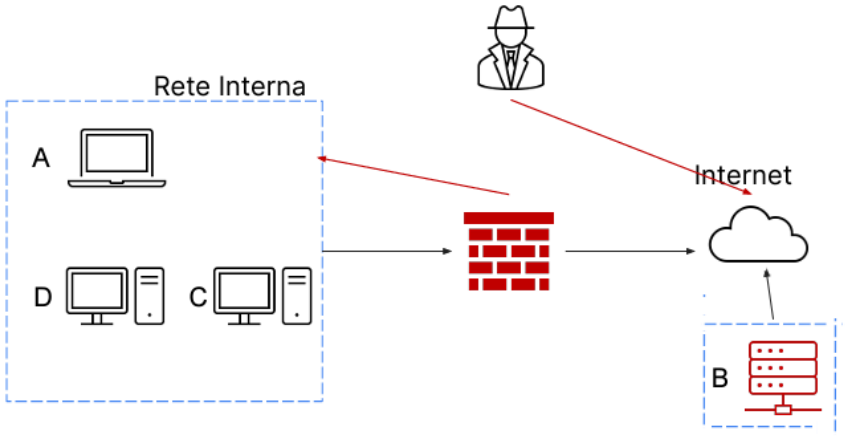
- Mostrate le tecniche di Isolamento and Rimozione del sistema B infetto
- Spiegate la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi

Svolgimento

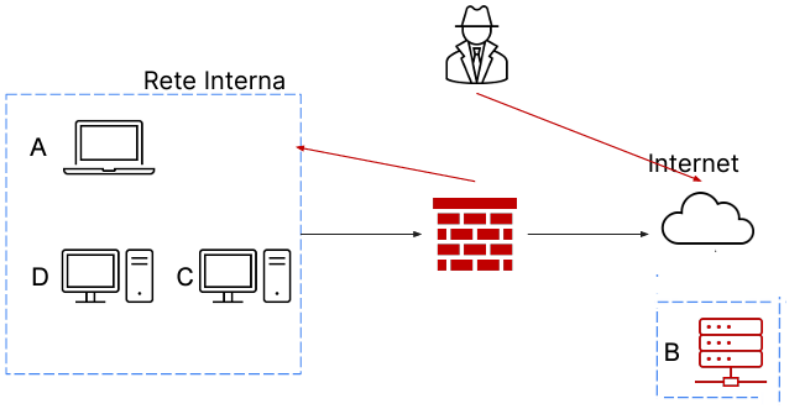
Parte I

Iniziamo a isolare e rimuovere il sistema B usando le due tecniche; Isolamento che consiste nel disconnessione del sistema B infetto, per non far accedere nella rete interna l'attaccante. Rimozione invece consiste nel non avere né accesso alla rete interna né a internet con la macchina infetta.

Isolamento



Rimozione



Parte II

Per la rimozione dei dati sensibili ci sono metodi che sono il Purge e Destroy. Il Purge elimina i dati sensibili rendendoli in irrecuperabili, lasciando intatto il supporto, mentre invece il Destroy elimina i dati sensibili ma distrugge anche il supporto fisico, ed è il metodo più efficace nel rendere le informazioni inaccessibili.