Pratica S9_L4

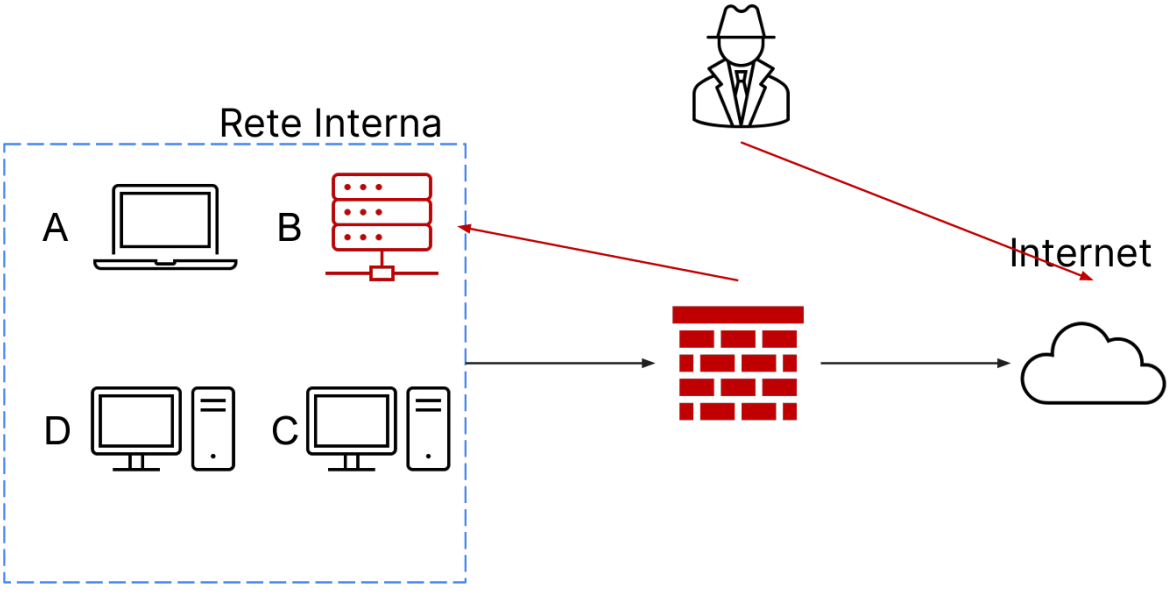
INCIDENT RESPONSE

L’esercizio odierno ci chiede di rispondere ad un attacco avviato via internet.

L’evento ha compromesso interamente un database contenente diversi dischi per lo storage, poiché il fatto è attualmente in corso, in qualità di team di CSIRT andiamo a spiegare :

- Le tecniche per ISOLARE e RIMUOVERE il sistema B INFETTO
- La differenza tra PURGE e DESTROY per eliminare le informazioni sensibili prima di smaltire i dischi compromessi
-

Sotto uno schema visivo della situazione



Dato che l’obiettivo è stato ormai compromesso nell’intero, e l’attacco è ancora in corso, ci troviamo in una situazione critica, pertanto procediamo nell’immediato ad ISOLARE il DATABASE B per evitare che vada a diffondere ulteriormente il problema nella nostra rete, lo facciamo tramite un software che prende il nome di PacketFence che, con un semplice click del mouse, va ad isolare la macchina, rendendola effettivamente impossibilitata a collegarsi con gli altri dispositivi, passeremo poi a staccare fisicamente tutti i cavi che si connettono al database per metterlo definitivamente offline.

Come secondo step dobbiamo rimuovere i dischi compromessi e smaltirli, quindi potremmo utilizzare due tecniche efficaci come PURGE che riporta i dischi all’impostazione di fabbrica o

scrive moltissime volte per coprire ogni precedente traccia, inoltre tramite forti magneti riesce ad annichilire le zone di memoria (che funzionano appunto magneticamente), altrimenti la tecnica del DESTROY che, dopo aver effettuato i passaggi del purge, va anche a disintegrare/polverizzare i materiali.

Nella nostra situazione una tecnica PURGE ci consente di cancellare i dati in modo efficiente e smaltire tutto con serenità.