S9 L4

Report esercizio “Incident Response Plan”

Giulia Salani

TRACCIA

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.

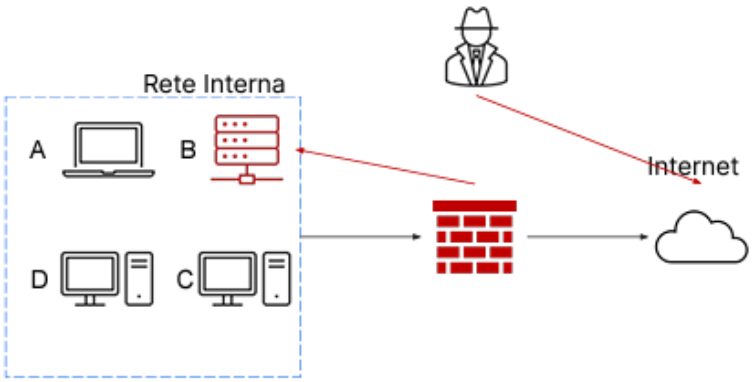
L'attacco è attualmente in corso e siete parte del team di CSIRT.

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

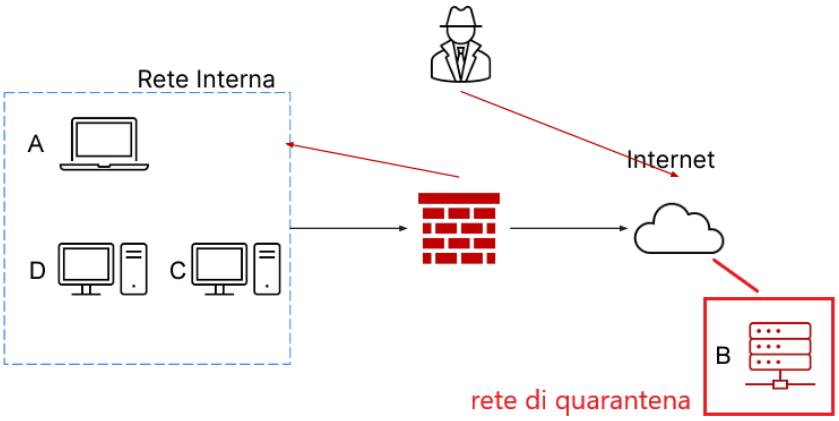


REPORT

MOSTRARE TECNICHE DI ISOLAMENTO E RIMOZIONE

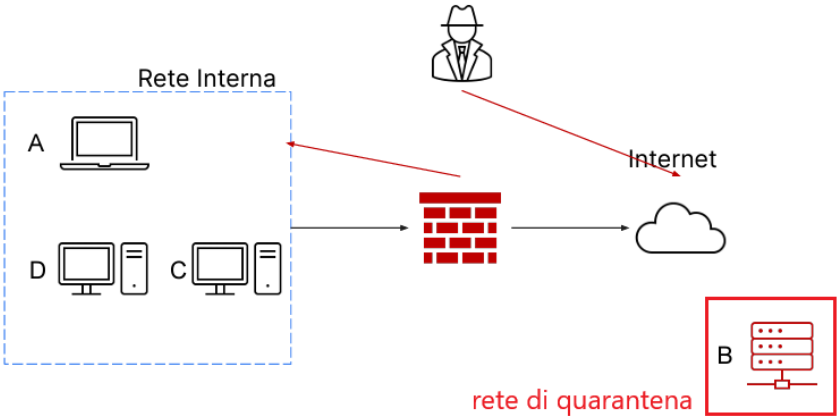
Tecniche di isolamento

L'isolamento consiste nella completa disconnessione del sistema infetto dalla rete, per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante:



Tecniche di rimozione

Il sistema è completamente rimosso sia dalla rete interna, sia dalla rete internet:



SPIEGARE LA DIFFERENZA FRA PURGE E DESTROY

Purge

- Processo che **implica la rimozione completa dei dati sensibili o compromessi dal dispositivo**.
- Questo metodo **mira a eliminare tutte le tracce di informazioni riservate, ripristinando il dispositivo** a uno stato in cui è sicuro da un punto di vista dei dati.
- È **spesso utilizzato quando si vuole preservare l'hardware** del dispositivo **e riutilizzarlo** successivamente.

Destroy

- Processo che **prevede la distruzione fisica del dispositivo** o dei suoi componenti critici.
- Questo metodo è più estremo e **viene scelto quando non è possibile garantire la completa eliminazione dei dati in modo sicuro** o quando la sicurezza a lungo termine è prioritaria rispetto al riutilizzo dell'hardware.
- La distruzione può avvenire tramite mezzi come triturazione, bruciatura o altre pratiche che rendono il dispositivo inutilizzabile.

In sintesi, **mentre "Purge" si concentra sulla rimozione sicura dei dati, "Destroy" implica la distruzione fisica del dispositivo** per garantire la protezione totale contro potenziali minacce legate a informazioni residue. La scelta tra i due dipende dalle esigenze specifiche di sicurezza e dalla futura destinazione del dispositivo.