ESERCIZIO W20D1

Andiamo ad applicare i concetti visti nel capitolo IRP(Incident response plan). Ipotizziamo una situazione di pericolo, come nella traccia:

- 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. Indicare anche Clear.

Isolamento

Per evitare tecniche di spostamento laterale e successivi attacchi agli endpoint della rete, isoliamo l'asset colpito in una rete di quarantena. Il sistema infetto risulterà ancora connesso a internet, ma non potrà più essere utilizzato per raggiungere gli altri computer.

Rimozione

Nel caso ci preoccupiamo ancora di più per la sorte del sistema infetto, possiamo scollegarlo da internet per mettere completamente a tacere l'attacco.

Durante la fase di recupero, vengono gestiti i dischi/sistemi attaccati. Si decide se smaltirli o riutilizzarli. A seconda della scelta si hanno diversi metodi:

- **Clear** = Prevede soluzioni logiche all'attacco. Si sovrascrivano costantemente i dati oppure si usa il factory reset.
- **Purge** = Si adottano, oltre alla rimozione di contenuti sensibili, azioni di rimozione fisica, come l'utilizzo di forti magneti per rendere le informazioni inaccessibili.
- **Destroy =** Oltre alle misure logiche e fisiche si ricorre all'atto di distruzione del sistema interessato. Parliamo di disintegrazione, polverizzazione e trapanazione.