ESERCITAZIONE W20D1 (1)

EPICODE

Esercizio
Incident response

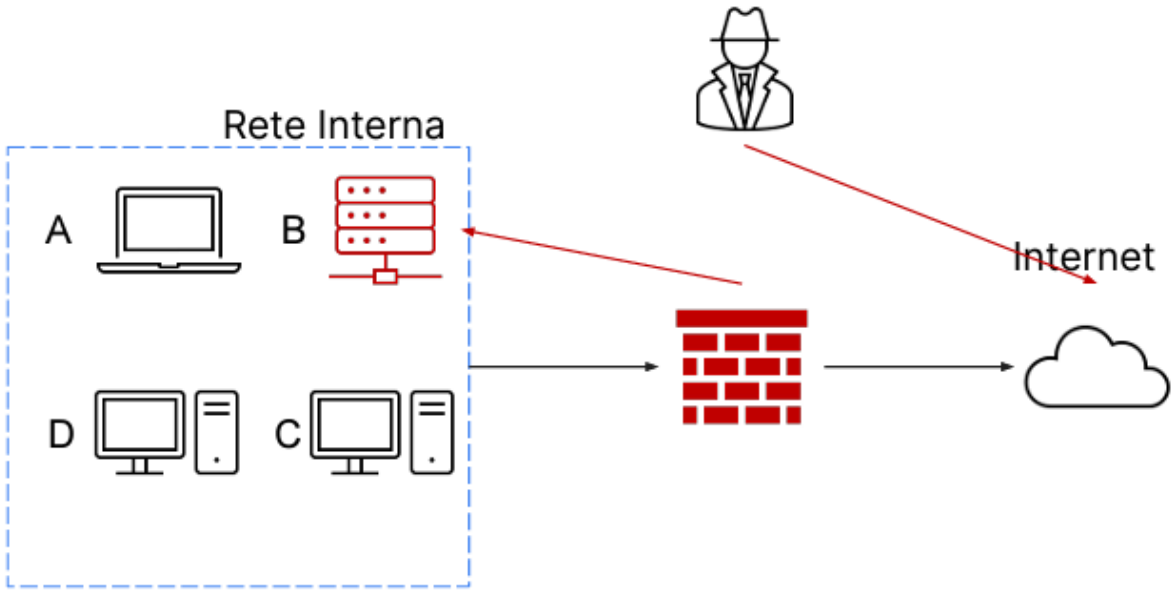
Traccia:

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. **Indicare anche Clear**



- **Isolamento**

Il primo procedimento da effettuare è isolare il **sistema b** infetto con la tecnica della segmentazione, ovvero separare il sistema compromesso dagli altri computer sulla rete, creando una rete di quarantena.

- **Rimozione**

In alcune circostanze, l'isolamento delle risorse compromesse potrebbe non essere sufficiente per garantire la sicurezza. In tali situazioni, si ricorre a una misura di contenimento più rigorosa,

che consiste nella completa disconnessione del sistema dalla rete interna e da Internet. In questo modo, l'attaccante non potrà accedere né alla rete interna né alla macchina infetta, fornendo un livello aggiuntivo di protezione.

- **Purge**

Nel processo di protezione dei dati sensibili, non solo si adotta un approccio logico, ma si impiegano anche tecniche di rimozione fisica. Queste includono l'uso di potenti magneti per rendere le informazioni irrecuperabili su specifici dispositivi.

- **Destroy**

Rappresenta l'approccio più radicale per lo smaltimento di dispositivi contenenti dati sensibili. Oltre ai metodi logici e fisici precedentemente menzionati, vengono impiegate tecniche di laboratorio come la disintegrazione, la polverizzazione dei supporti ad alte temperature e la trapanazione. Benché estremamente efficace nel rendere le informazioni del tutto inaccessibili, questo metodo richiede un considerevole investimento economico.

- **Clear**

Clear è un processo in cui il dispositivo viene completamente privato dei suoi contenuti mediante tecniche "logiche". Questo può includere l'utilizzo di un approccio di tipo "read and write", in cui il contenuto viene sovrascritto più volte, oppure l'esecuzione della funzione di "factory reset" per riportare il dispositivo allo stato iniziale.