


# Report

Casistica :



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**

3

Nella casistica qui presentata è necessario utilizzare la tecnica dell'isolamento e della rimozione totale del sistema infetto. Una volta isolato e messo in quarantena il computer.

Tramite la tecnica di isolamento dunque andiamo a isolare il sistema infetto e quindi impedire all'attaccante di avere accesso ad altri computer nella rete interna dell'azienda. Con la rimozione all'attaccante viene bloccato pure l'accesso alla macchina infettata.

Una volta eseguiti questi due passaggi possiamo alla eliminazione delle informazioni sensibili.

Per l'eliminazione dei dati vi sono diversi metodi tra i quali :

Il metodo Purge : In questo metodo il soggetto non solo procede con la formattazione come nel caso del clear , ma si procede anche all'utilizzo di dispositivi che rendono le informazioni inaccessibili.

Il metodo destroy: Nel caso invece del destroy si provvede proprio a distruggere il dispositivo fisicamente ovviamente il tutto in un ambiente controllato e sicuro per poter fare cio