Gestione database infetto

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 del sistema B infetto:

Come primo passaggio isolerei la rete , disconnettendo il sistema infetto dalla rete principale per prevenire ulteriori danni (come malware che camminano tra le reti, o ulteriori accessi non autorizzati).
Gestirei come seconda cosa un contenimento, consentendo un accesso limitato per indagini e bonifiche future.

Rimozione del sistema B infetto:

Inizialmente userei uno spegnimento controllato del sistema per preservare i dati che serviranno per le indagini forense, come seconda cosa andrei a rimuovere fisicamente i dischi o il sistema per ulteriori indagini in ambienti piu' sicuri.
Proseguirei con la pulizia e il ripristino con degli strumenti di bonifica e ripristinare i dati da backup sicuri.

Differenze tra Purge, Destroy, Clear:

Purge: Questa tecnica consiste nell'eliminazione delle informazioni sensibili da un dispositivo in modo tale che sia difficile, ma non impossibile, recuperarle.

Destroy: Implica la distruzione fisica del dispositivo contenente le informazioni sensibili.
Questa tecnica implica la perdita totale dei dati.

Clear: Consiste nella rimozione delle informazioni sensibili in modo tale che non possono essere recuperate utilizzando normali tecniche di recupero.