Esercitazione WEEK 20 D1 (1)

Incident Response

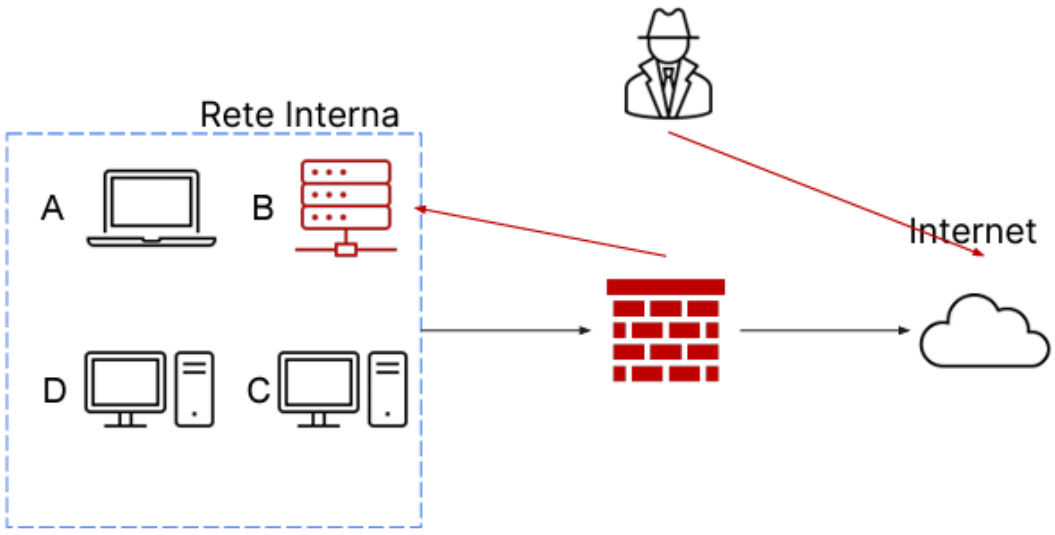
Ettore Farris

Descrizione sintetica

Con riferimento alla figura di sotto, 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



Svolgimento

- **Isolamento**

Per ridurre gli impatti è opportuno isolare l'incidente in modo che il sistema infetto non possa compromettere nessun altro asset tramite, ad esempio, movimenti laterali.

Una possibile tecnica è la **segmentazione della rete** finalizzata ad isolare l'attacco dalla rete creando una rete ad hoc, che viene chiamata generalmente **rete di quarantena.**

Tuttavia è probabile che questo non basti. Per avere un contenimento maggiore, si utilizza la tecnica dell'**isolamento**, che consiste nella completa disconnessione del sistema infetto dalla rete: in questo modo si restringe ancor di più l'accesso alla rete interna da parte dell'attaccante.

- **Rimozione del sistema infetto**

A seguito dell'attività di contenimento descritta sopra, è necessario rimuovere ogni traccia dell'incidente. Il sistema attaccato, essendo costituito da dei dischi di storage, necessità di un'attività di smaltimento o recupero dei dischi. Le tecniche per smaltire o recuperare i dischi sono:

- *Purge*: rimozione dei dati con metodi fisici, come l'utilizzo di forti magneti per rendere i dati inaccessibili.
- *Destroy*: distruzione totale del disco mediante disintegrazione, polverizzazione dei media ad alte temperature, trapanazione.
- *Clear*: rimozione dei dati con tecniche logiche come il *factory reset* o l'approccio *read and write* (il contenuto viene sovrascritto più e più volte)