

Esercitazione W20D1 - Pratica 1

Incident Response

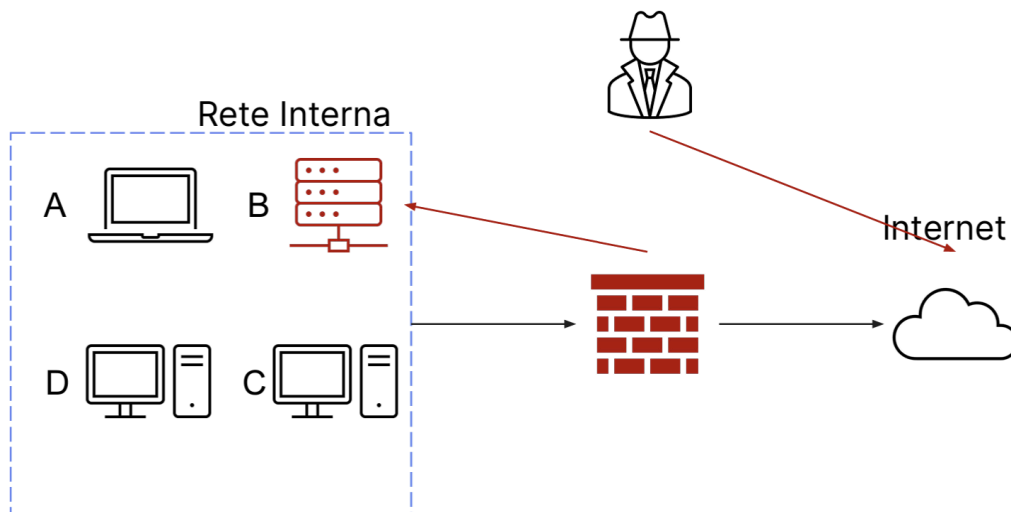
Fabio Benevento - 19/03/2024

Traccia

Con riferimento alla figura, 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.

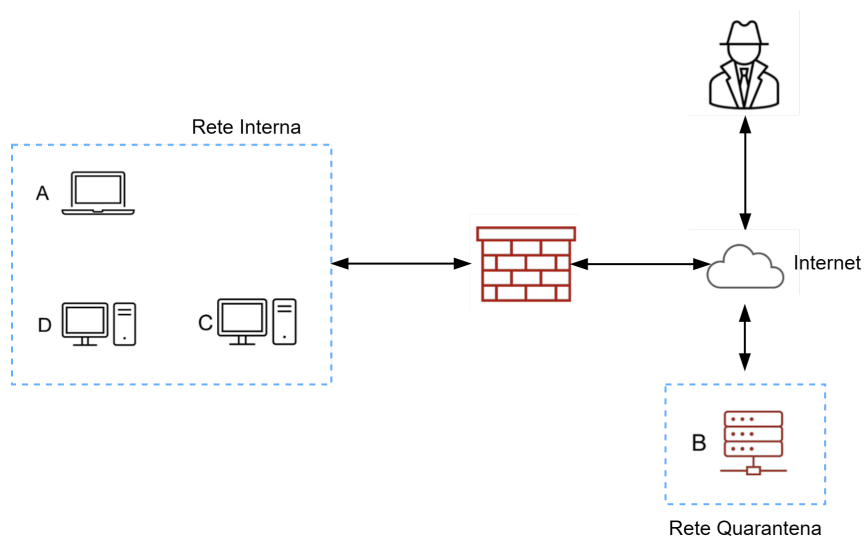
- Mostrate le tecniche di: I) Isolamento II) Rimozione del sistema B infetto
- Spiegate la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. Indicare anche Clear



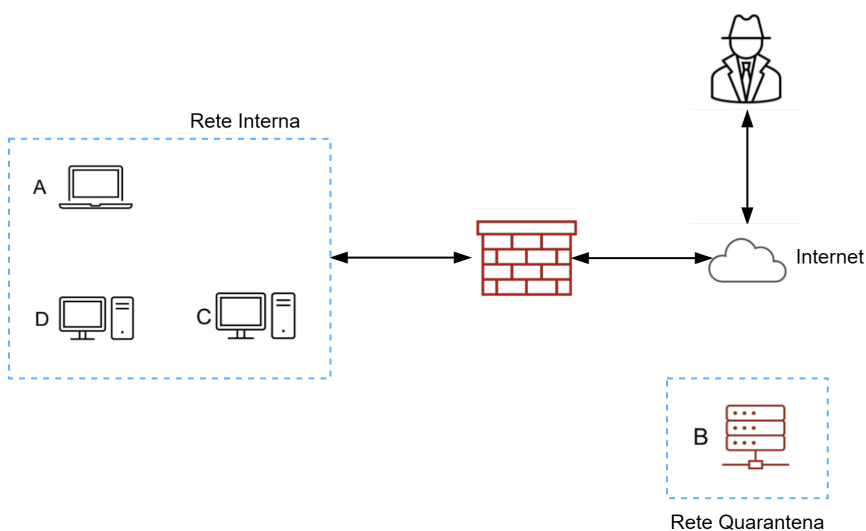
Implementazione


- Mostrate le tecniche di: I) Isolamento II) Rimozione del sistema B infetto

Nella tecnica di isolamento del sistema compromesso, esso viene collocato in una nuova sottorete mediante segmentazione, detta rete di quarantena, al fine di evitare che il virus possa propagarsi negli altri dispositivi della rete. La connessione ad Internet viene comunque mantenuta



Adottando invece la tecnica della rimozione, esso viene completamente scollegato dalla rete, e il sistema infetto non ha accesso ad Internet.





- Spiegate la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. Indicare anche Clear

Nella tecnica di smaltimento/pulizia dei dischi compromessi Clear, vengono adottate delle tecniche “logiche” di pulizia con riscritture multiple del device o l'esecuzione del factory reset.

Con la tecnica Purge, vengono non solo adottate tecniche logiche ma anche fisiche, mediante potenti magneti per smagnetizzare il device.

Infine la tecnica Destroy è la più invasiva in quanto vengono usate tecniche come la polverizzazione o la trapanazione per la distruzione del device rendendolo inutilizzabile.