S9L4

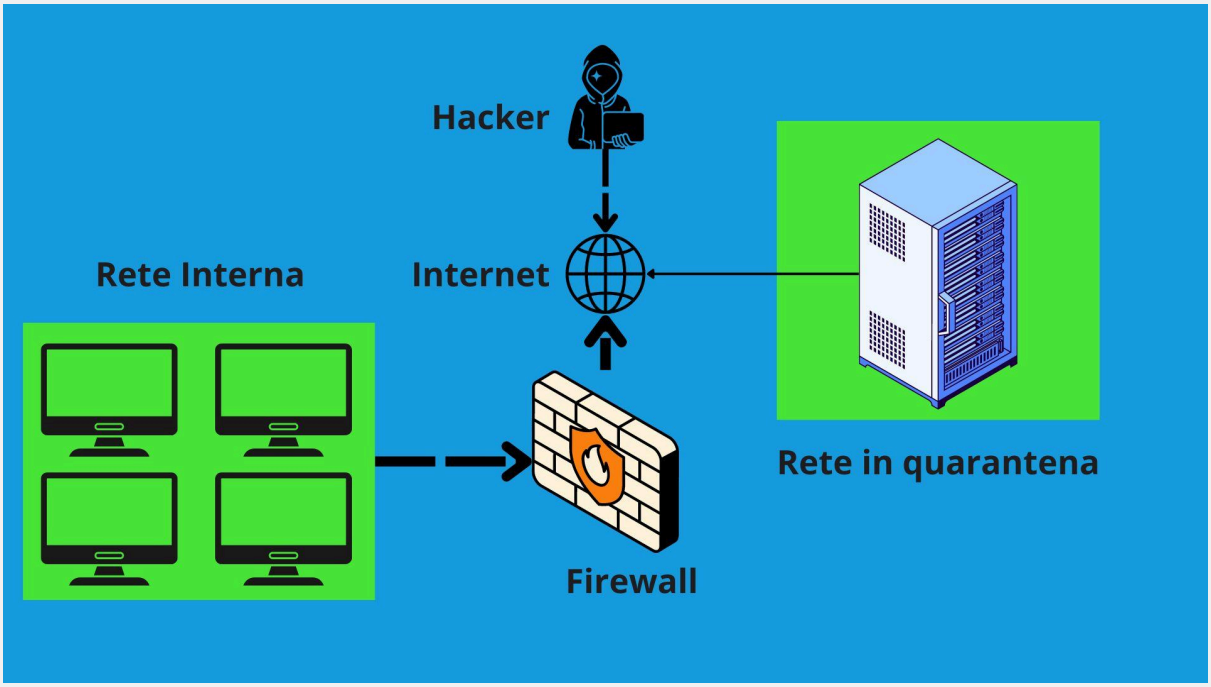
Traccia:

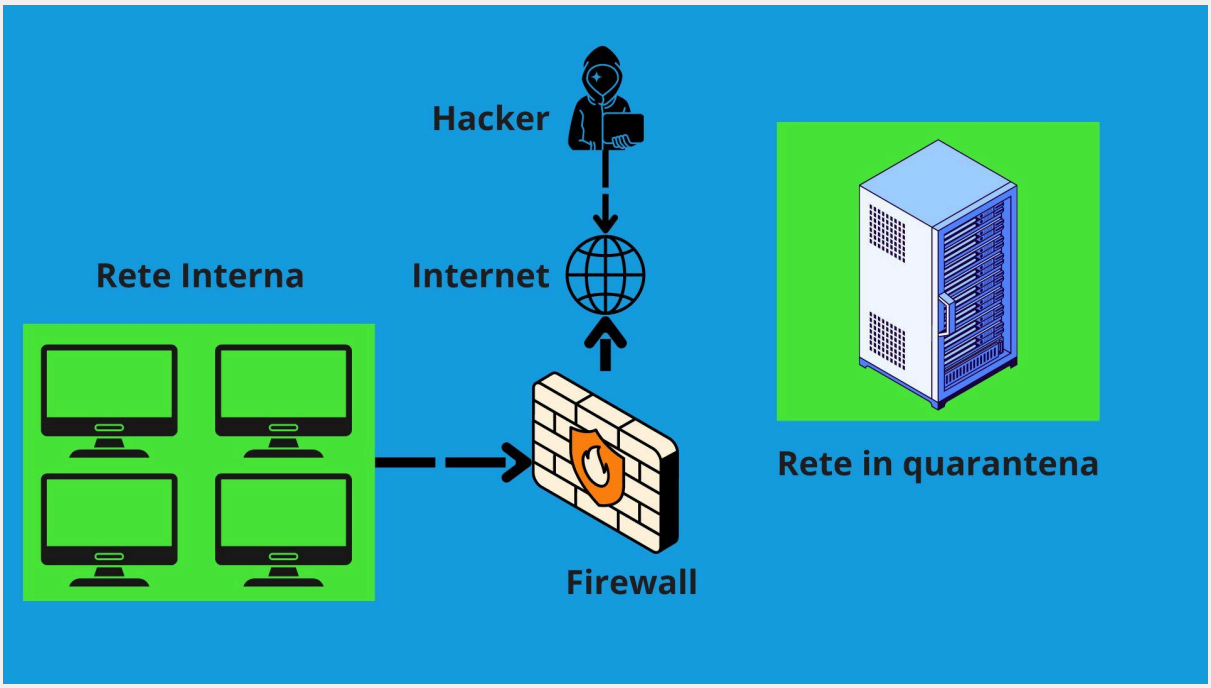
Con riferimento alla figura in slide 4, il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite internet.
L'attacco è attualmente in corso e siete parte del team di CSIRT.
Rispondere ai 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

Nelle seguenti slide sono mostrati degli esempi di isolamento e rimozione di un dispositivo infetto da una rete.
In entrambi i casi la rete è stata segmentata per limitare la diffusione di malware infetto alla rete interna e per separare l'elemento infetto dalla rete interna.
Nel caso dell'isolamento il server infetto è stato spostato in una rete diversa chiamata "Rete di quarantena", in questo modo il server infetto non può più comunicare con le macchine presenti nella rete interna ma può ancora comunicare con internet.

Nel caso della rimozione il server infetto è stato spostato in una rete diversa chiamata "Rete di quarantena", però a differenza dell'isolamento in questo caso il server infetto è stato tagliato fuori da qualsiasi comunicazione e non può connettersi neanche ad internet.


Hacker
Rete Interna
Internet
Rete in quarantena
Firewall


Hacker
Rete Interna
Internet
Rete in quarantena
Firewall

Differenza tra Purge e Destroy:

Quando vogliamo assicurarci che dei file contenuti nei dischi rigidi diventano inaccessibili ed impossibili da reperire possiamo optare per diversi metodi, vediamo in dettaglio due di questi.

Metodo Purge:

Questa tecnica prevede l'utilizzo di magneti molto potenti per smagnetizzare il disco rigido e renderlo illeggibile ed eliminando ogni possibilità di scriverci ulteriori dati al di sopra.

Metodo Destroy:

Questa tecnica prevede la distruzione fisica del disco rigido tramite incenerimento, alla fine del processo non rimane altro che cenere e di conseguenza non sarà possibile effettuare alcun tipo di analisi per tentare di recuperare i dati precedentemente scritti sull'hard disk.