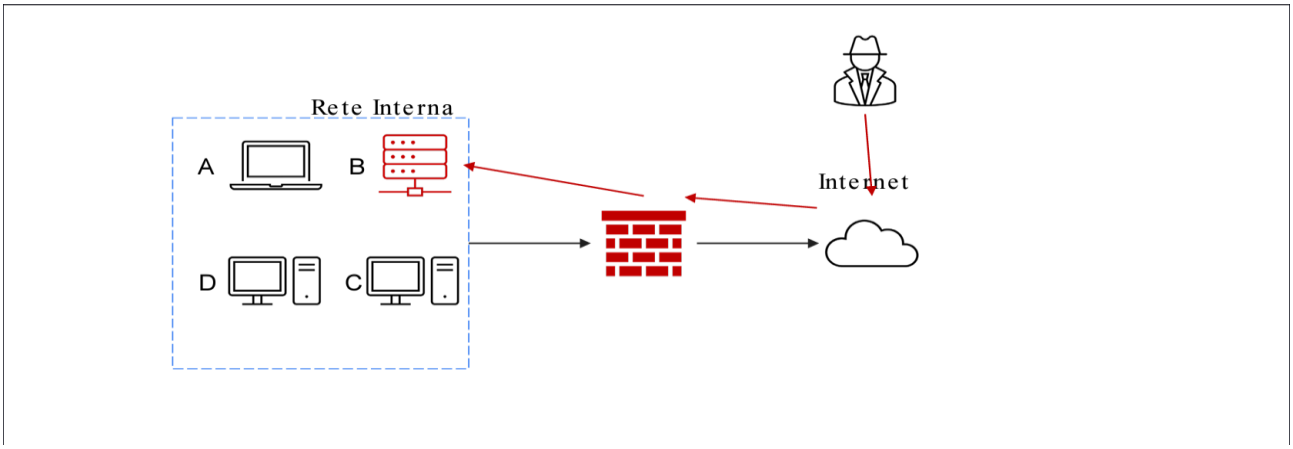
REPORT CS1024

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 Destroyer l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. Indicare anche Clear



Isolamento

La tecnica di isolamento consiste nel disconnetere completamente il sistema infetto e metterlo in quarantena in modo tale da non permettere all'attaccante di eseguire azioni malevole. Questo metodo e' molto efficace perche' permette di prendere un po' di tempo mentre si effettuano delle valutazioni sulla difesa del sistema.

Rimozione

La tecnica di rimozione avviene quando si decide che il sistema debba essere eliminato completamente dalla rete perche' la sola quarantena non basta. In questo modo l'attaccante non ha piu il controllo della sistema infetto.

PURGE, DESTROY & CLEAR

PURGE: E’ una manovra che si adotta quando i vanno a cancellare i contenuti sensibili, che possono sfociare addirittura nella rimozione fisica del dispositivo.

DESTROY: Questo approccio si adotta nel momento in cui il Purge non basta, si effettuano quindi delle azioni tecniche di laboratorio con lo scopo di disintegrare o polverizzare i dispositivi infetti. Ovviamente non essendo una tecnica semplice da finalizzare il costo della suddetta sara’ molto elevato rispetto ad un purge.

CLEAR:In questo caso il dispositivo viene completamente ripulito seguendo le azioni logiche possibili. Una delle tecniche piu’ utilizzate e’ infatti quella di resettare il dispositivo ai dati di fabbrica, in modo tale da cancellare e pulire il dispositivo e riportarlo appunto nel suo stadio iniziale.