domenica 17 novembre 2024 21:21

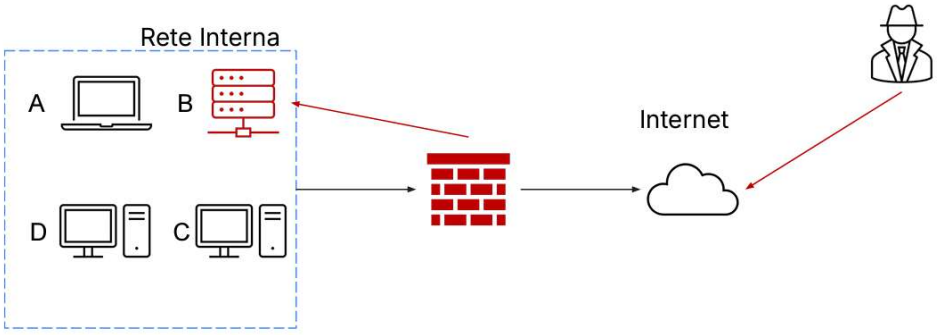
**Traccia:**

**Con riferimento alla figura nella prossima slide, 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 e accedere al sistema tramite Internet.**

**L'attacco è attualmente in corso e siete parte del team di CSIRT.**

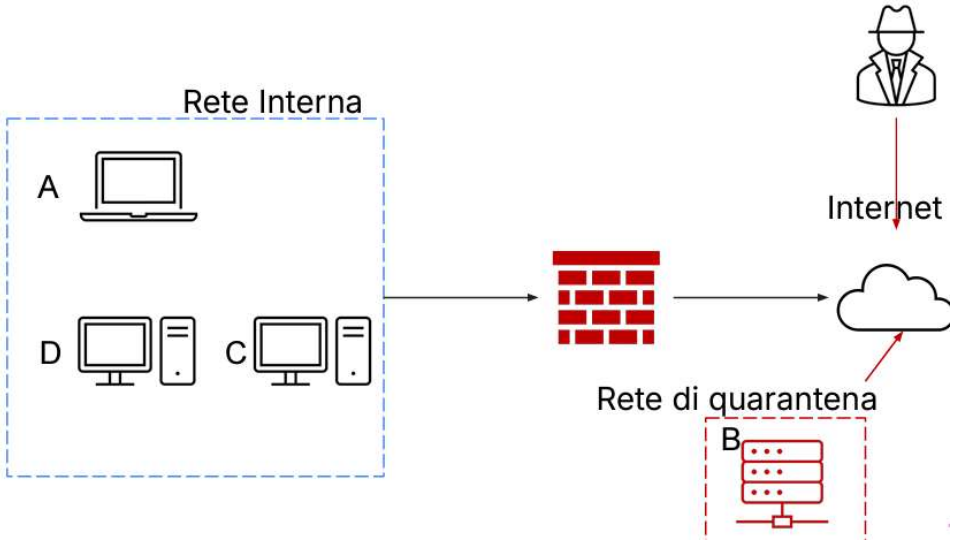
**Rispondere ai seguenti quesiti.**

- **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**



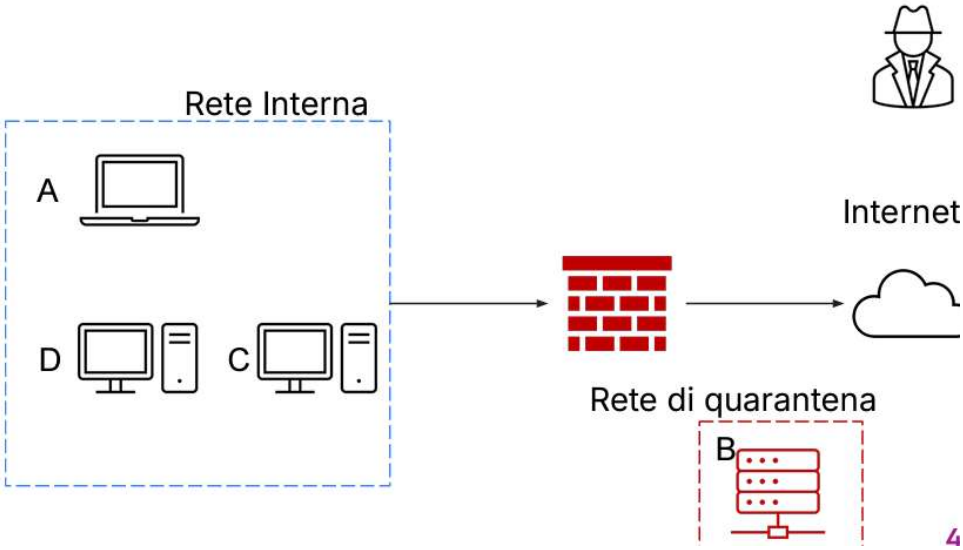

## I) Isolamento

La tecnica di isolamento permette di isolare un sistema infetto restringendo l'accesso dell'attaccante alla rete interna. Tuttavia il sistema infetto sarà ancora accessibile dall'attaccante via internet




## II) Rimozione

La tecnica di Rimozione elimina completamente il sistema dalla rete, rendendolo inaccessibile sia da rete interna che da internet. Questo approccio restringe l'accesso alla rete interna da parte dell'attaccante che non avrà nemmeno più accesso al sistema infetto.




**Purge:**

Si tratta della rimozione dei dati su un disco in modo permanente, rendendoli irrecuperabili anche attraverso metodi di recupero avanzati.

Include tecniche come la *sovrascrittura multipla con metodi approvati* (ad esempio, standard DoD 5220.22-M o NIST 800-88).
Può utilizzare strumenti hardware o comandi di *secure erase* che accedono direttamente al firmware del disco.
A volte implica anche la smagnetizzazione (degaussing), che cancella i dati

alterando il campo magnetico del disco.

L'obbiettivo è quello di prevenire qualsiasi recupero dei dati tramite tecnologie avanzate. Questa è l'opzione consigliata per dischi destinati a essere riciclati o trasferiti all'esterno.

**Destroy:**

Comporta la distruzione fisica del disco per eliminare completamente qualsiasi possibilità di recupero.

Distruzione meccanica (triturazione, perforazione o frantumazione).
Incenerimento o uso di sostanze chimiche corrosive.

Rimuovere fisicamente ogni traccia dei dati.
Adatto per dispositivi con dati altamente sensibili che devono essere definitivamente smaltiti.
Questo metodo è sicuramente il più efficace per rendere le informazioni inaccessibili ma è anche quello che comporta un effort in termini economici maggiore.

**Clear:**

il dispositivo viene completamente ripulito dal suo contenuto con tecniche di rimozione logica dei dati da un disco, in modo che non siano più facilmente accessibili.

Utilizza comandi come delete o format, o tecniche di sovrascrittura standard (ad esempio, sovrascrivere i dati una o più volte con pattern come zero, uno, o valori casuali).
Può essere eseguito tramite software come *DBAN* o strumenti nativi del sistema operativo.

Ha l'obbiettivo di impedire l'accesso casuale ai dati con metodi standard anche se possono ancora essere recuperati con tecniche avanzate come l'analisi forense del disco.
Questo metodo è più adatto per dischi da riutilizzare in ambienti interni di bassa sensibilità.