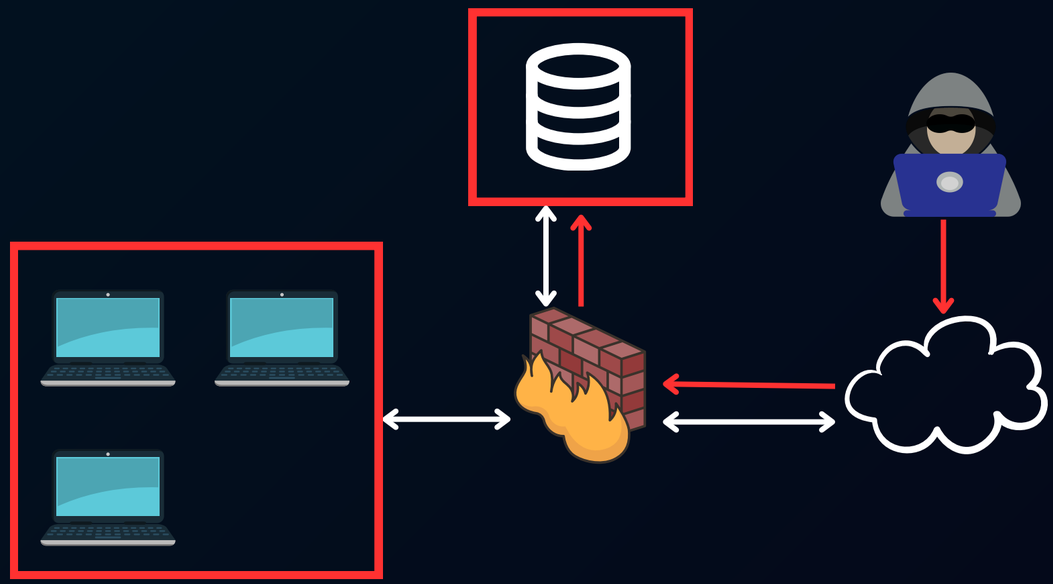
Rispondere ai seguenti quesiti

- 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

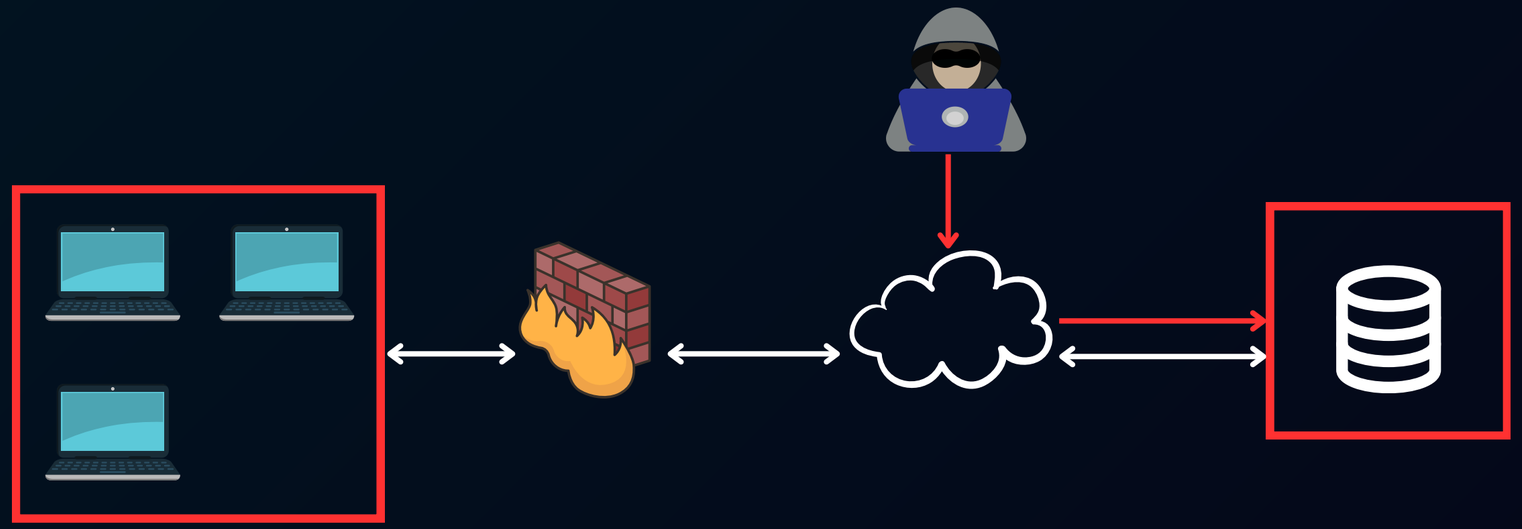
FASE 1: QUARANTENA

Disconnettere il database dalla rete per impedire la diffusione dell’attacco e compromettere altre macchine e metterlo in una “rete di quarentena”.
Utilizzare strumenti di analisi forense per esaminare il database e identificare tutti i punti di compromissione e verificare i log di accesso e utilizzo per tracciare le attività sospette.



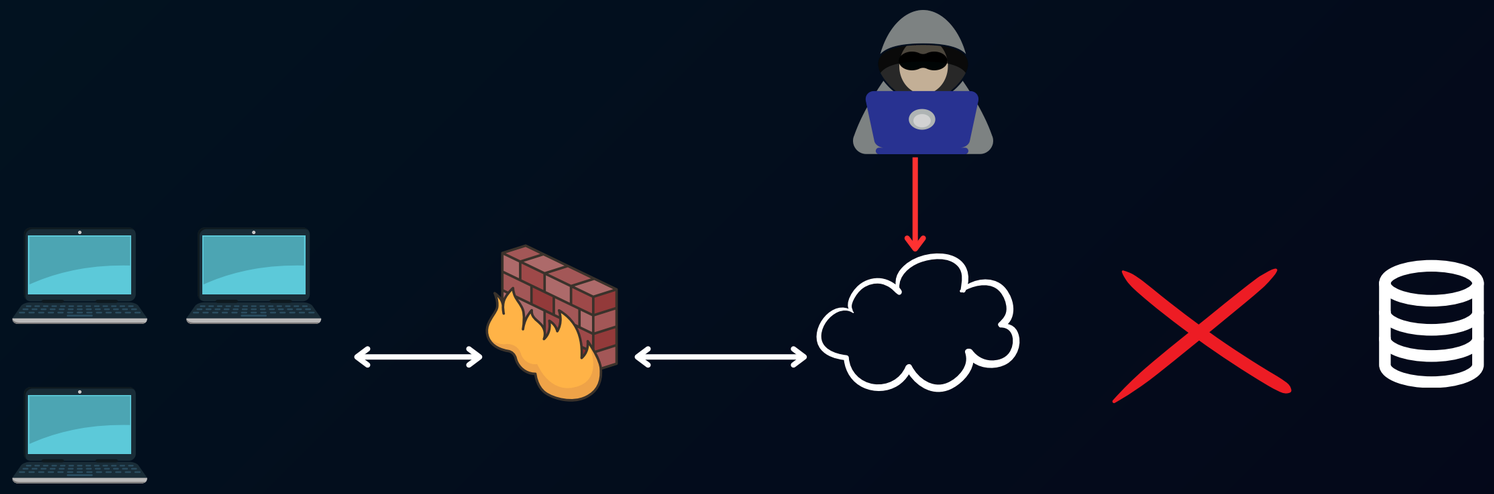
FASE 2: ISOLAMENTO

Rimuovere il database dalla rete interna ma lasciarlo comunque accessibile ad internet, in questo modo l’attaccante avrà accesso solo al database ormai compromesso ma non potrà accedere in alcun modo alla rete interna



FASE 3: RIMOZIONE

Scollegare fisicamente il database per isolarlo completamente e analizzarlo in un ambiente di sandbox per comprendere il comportamento dell’attacco e i metodi di infezione.



FASE 4: RECUPERO

Ripristinare il sistema con un backup pulito, aggiornare le patch di sicurezza e il software del database

Verificare l’integrità del database affinchè non ci siano tracce o attività sospette

Implementare un monitoraggio continuo, ad esempio con un SIEM

Il termine purge si riferisce alla rimozione di dati in modo tale che non possano essere recuperati attraverso alcun tipo di attacco su software o hardware, se non con l'uso di tecniche straordinarie. Purge è un metodo di pulizia più approfondito rispetto alla semplice cancellazione dei dati.

Tecniche di Purge:

- Overwrite (Sovrascrittura): Scrivere dati casuali o schemi specifici più volte sui dati esistenti.
- Block Erase: Per i dispositivi di memorizzazione basati su memoria flash, cancellare i blocchi di memoria.
- Cryptographic Erase: Eliminare la chiave crittografica utilizzata per proteggere i dati, rendendo i dati stessi incomprensibili.

Il termine destroy si riferisce alla distruzione fisica dei supporti di memorizzazione, rendendo impossibile il recupero dei dati con qualsiasi metodo, inclusi quelli straordinari.

Tecniche di Destroy:

- Shredding (Frammentazione): Ridurre il supporto di memorizzazione in piccoli pezzi.
- Incineration (Incenerimento): Bruciare il supporto fino a ridurlo in cenere.
- Crushing (Frantumazione): Schiacciare il supporto di memorizzazione fino a renderlo inutilizzabile.
- Degaussing: Applicare un forte campo magnetico per smagnetizzare i dischi rigidi, distruggendo i dati memorizzati.

Il termine clear si riferisce alla rimozione dei dati in modo tale che non possano essere recuperati attraverso mezzi standard, come software di recupero dati commerciali. Tuttavia, potrebbe essere possibile recuperare i dati con tecniche avanzate.

Tecniche di Clear:

- Deletion (Cancellazione): Eliminare i file o formattare il dispositivo di memorizzazione, il che rende i dati non facilmente accessibili.
- Overwrite (Singola Sovrascrittura): Scrivere dati casuali una sola volta sui dati esistenti.