

Incident response

Esercizio S9/L4


Indice

- Traccia
- Schema iniziale
- Tecniche di isolamento
- Tecniche di rimozione
- Purge vs Destroy
- Tecnica Clear
- Conclusioni



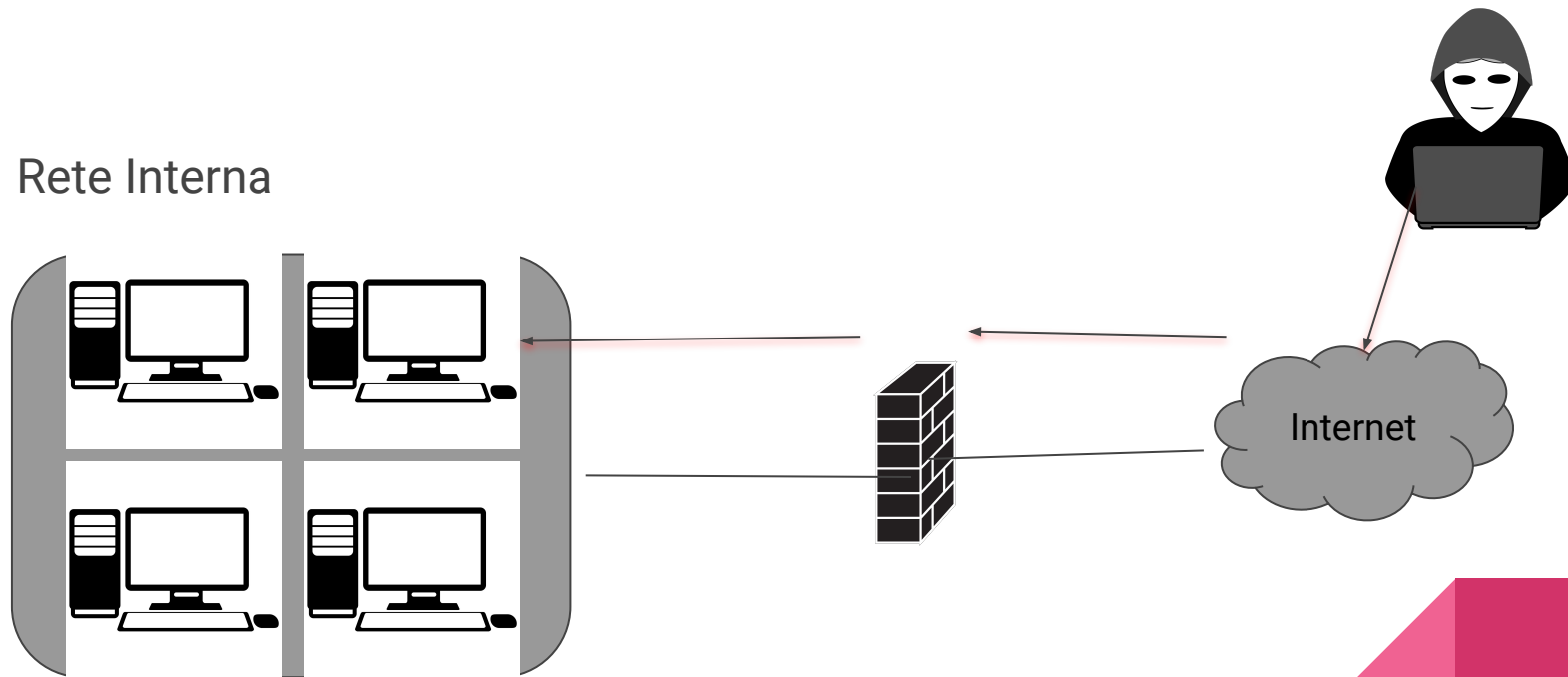
Traccia

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:

- 1) Isolamento
 - 2) Rimozione del sistema B infetto
 - 3) Spiegate la differenza tra Purge e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi.
 - 4) Indicare anche Clear
- 

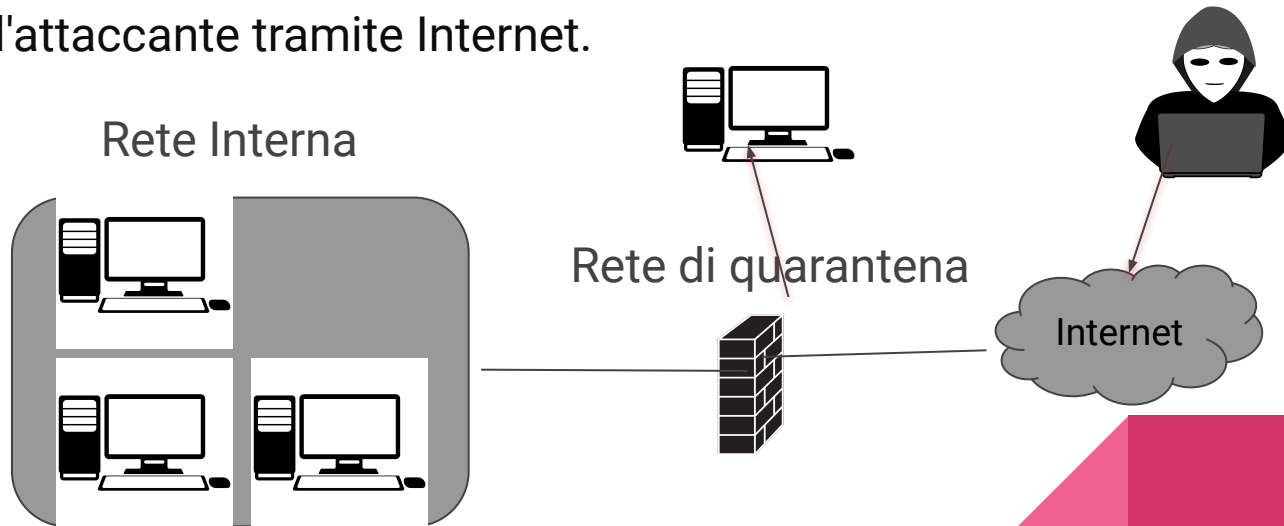
Schema iniziale

Rete Interna



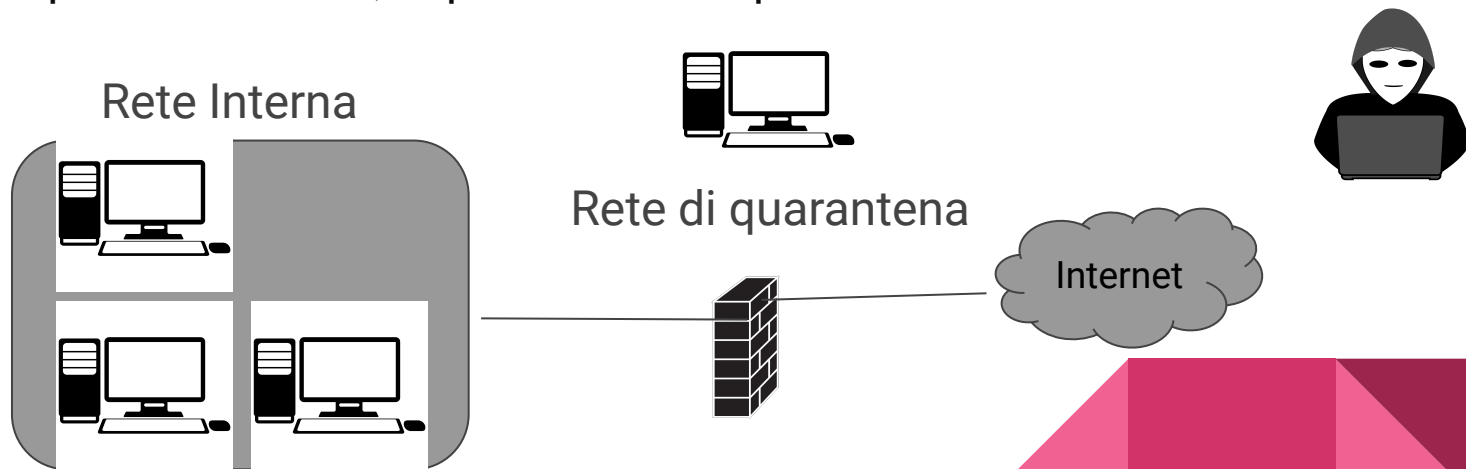
Tecniche di isolamento

La tecnica di isolamento consente di separare un sistema infetto, limitando l'accesso dell'attaccante alla rete interna. Inoltre, il sistema infetto rimarrà accessibile all'attaccante tramite Internet.



Tecniche di rimozione

La tecnica di Rimozione cancella il sistema dalla rete, rendendolo completamente inaccessibile sia dalla rete interna che da Internet. Questo metodo limita l'accesso alla rete interna per l'attaccante, il quale non avrà più alcun accesso al sistema infetto.



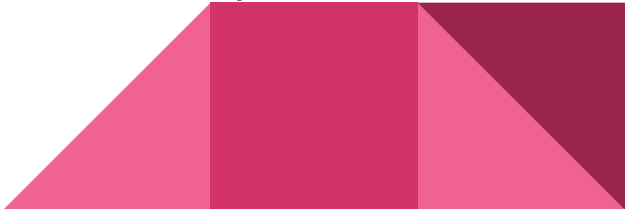
Purge vs Destroy

La tecnica di "purge" è un processo che coinvolge l'implementazione di misure, sia logiche che fisiche, per garantire l'eliminazione definitiva dei dati memorizzati su un disco o dispositivo di archiviazione. Questo metodo è finalizzato ad assicurare che i dati sensibili o riservati non siano più recuperabili in nessuna forma una volta eliminati. Le misure logiche possono comprendere l'operazione di sovrascrittura dei dati o l'applicazione di crittografia, mentre le misure fisiche possono includere la demagnetizzazione del supporto di archiviazione.



Purge vs Destroy

La tecnica "destroy" è un metodo estremamente radicale impiegato per rendere definitivamente inaccessibili i dati conservati su un disco o dispositivo di archiviazione. Questo approccio comporta l'adozione di misure fisiche molto invasive che possono includere la completa distruzione dell'hardware stesso. Di conseguenza, il dispositivo viene danneggiato irreparabilmente, rendendo impossibile il recupero dei dati in qualsiasi forma. La tecnica "destroy" viene comunemente adottata quando è necessario eliminare completamente e irreversibilmente un dispositivo di archiviazione, ad esempio per garantire la totale sicurezza dei dati sensibili o riservati prima dello smaltimento del dispositivo.



Tecnica clear

Questo metodo comporta la pulizia completa del dispositivo dai suoi dati utilizzando tecniche "logiche". Un esempio comune è l'approccio di tipo read-and-write, in cui il contenuto viene sovrascritto più volte. In alternativa, si può ricorrere alla funzione di "factory reset" per riportare il dispositivo allo stato iniziale.



Conclusioni

In conclusione, non esiste un metodo migliore in assoluto, ma piuttosto una scelta che dipende dalle esigenze di sicurezza e dalle circostanze specifiche. È importante valutare attentamente i vantaggi e gli svantaggi di ciascun metodo prima di prendere una decisione.





Grazie