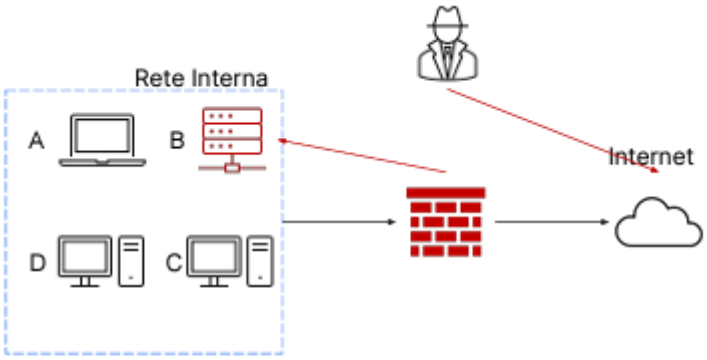
W20D1

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

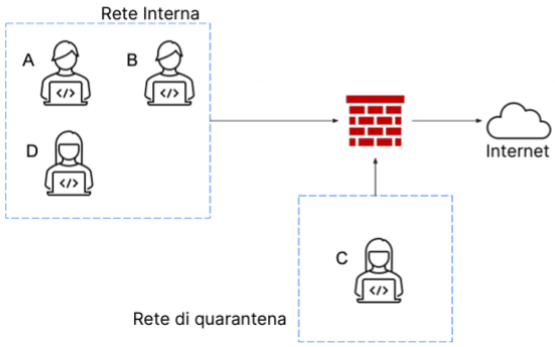


.1 FASE ISOLAMENTO

Durante un attacco informatico (incidente di sicurezza) dopo un approfondita fase d analisi, si cerca di contenere il danno quanto piu possibile . In questa fase scatta l attivita di contenimento del danno , ovvero si cerca di isolare il prima possibile il sistema / macchina per evitare uno spostamento laterale e lo scalo dei privilegi , impedendo cosi alla minaccia identificata di diffondersi e compromettere tutta la rete.

Diverse sono poi le varianti di isolamento:

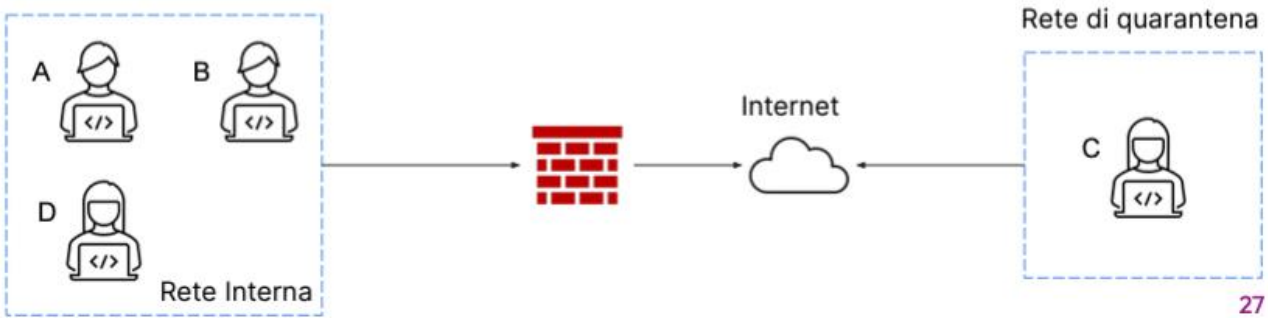
Rete di quarantena:



e possibile isolare la macchina infetta tramite la segmentazione della rete, ovvero spostare (l infetto)dalle macchine presenti in rete creando una rete ad hoc .

Attenzione: nonostante cio la macchina infetta continua ad essere comunque collegata sia al firewall che alla rete internet, nulla impedisce al malware di spostarsi sulla rete “sana”

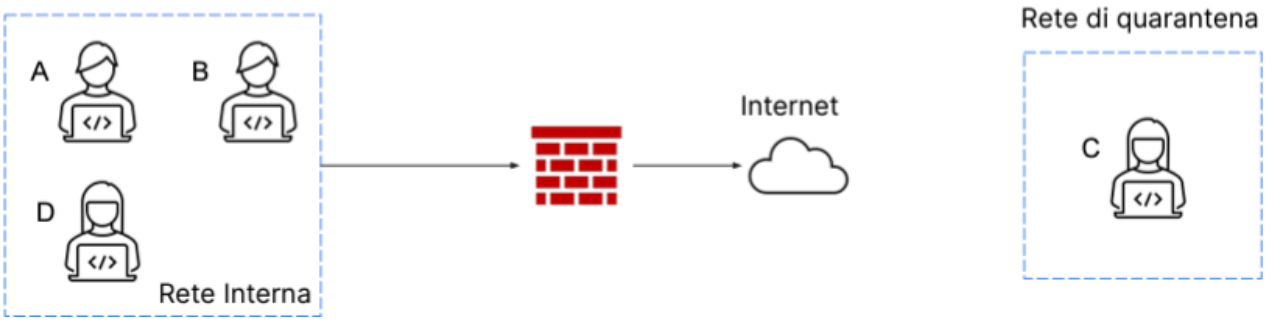
Un livello di contenimento maggiore puo essere la tecnica dell isolamento :



Con questa tecnica come vediamo in figura, viene creata una rete ad hoc per la macchina infetta , completamente esterna senza nessun contatto con la rete da proteggere. Nonostante cio la macchina in isolamento resta sempre attaccata alla rete internet e quindi in contatto con l attaccante .

Nel caso in esempio, essendo un server la macchina infetta ,nessuna delle due tecniche e adatta in quanto entrambe offrono comunque una connessione ad internet, e cio permetterebbe comunque al attaccante di sottrarci dei dati .

L unica azione da ritenersi valida e la rimozione del server sia dalla rete interna che dalla rete internet.



In questo scenario l attaccante non avra ne accesso alla rete interna ne tantomeno alla macchina infetta.

In fine si puo procedere o al recupero del dispositivo infetto o la totale distruzione dei sui hard disc

(impedendo cosi un qualsiasi tipo diffusione dei dati sensibili .)

Generalmente, possiamo individuare tre opzioni per la gestione dei media contenenti informazioni sensibili:

- Clear: il dispositivo viene completamente ripulito dal suo contenuto con tecniche «logiche». Si utilizza ad esempio un approccio di tipo read and write dove il contenuto viene sovrascritto più e più volte o si utilizza la funzione di «factory reset» per riportare il dispositivo nello stato iniziale.

-Purge: si adotta non solo un approccio logico per la rimozione dei contenuti sensibili, come visto nel caso di clear, ma anche tecniche di rimozione fisica come l'utilizzo di forti magneti per rendere le informazioni inaccessibili su determinati dispositivi

-Destroy: è l'approccio più netto per lo smaltimento di dispositivi contenenti dati sensibili. Oltre ai meccanismi logici e fisici appena visti, si utilizzano tecniche di laboratorio come disintegrazione, polverizzazione dei media ad alte temperature, trapanazione. Questo metodo è sicuramente il più efficace

per rendere le informazioni inaccessibili ma è anche quello che comporta un effort in termini economici maggiore.