Manuel Di Gangi

S9_L4

Incident response

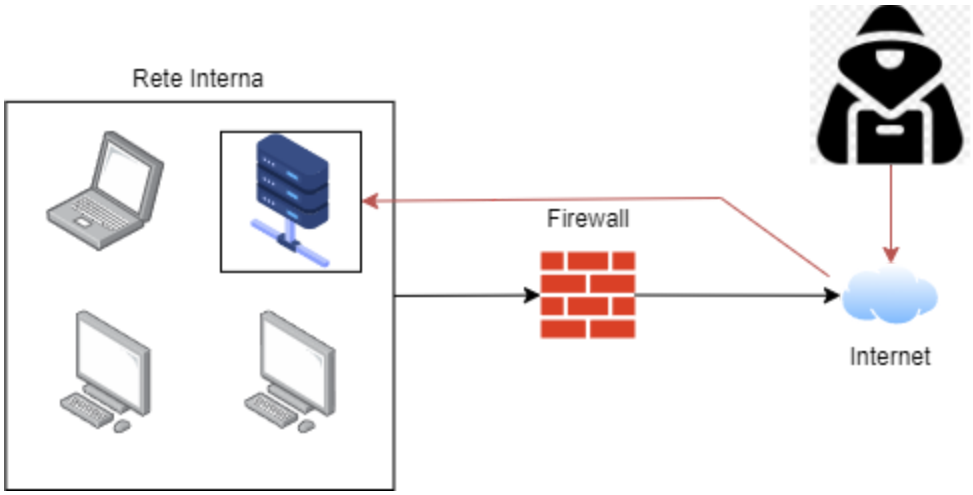
21 marzo 2024

INDICE

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:
  - Isolamento
  - Rimozione del sistema infetto
- Spiegate la differenza tra Purgee e Destroy per l'eliminazione delle informazioni sensibili prima di procedere allo smaltimento dei dischi compromessi. Indicare anche Clear



1. Nozioni Teoriche

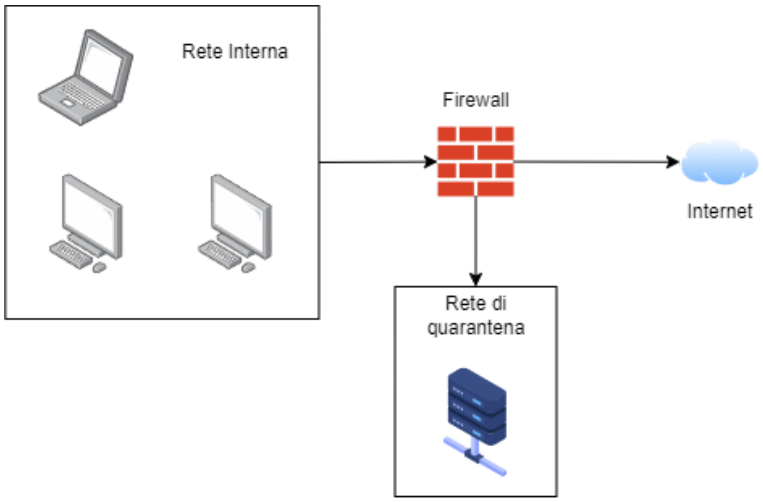
La compromissione di un sistema informatico si verifica quando un'entità esterna o interna riesce ad accedere, manipolare o danneggiare il sistema senza autorizzazione. Questo può avvenire attraverso varie forme di attacchi informatici come hacking, malware, phishing, o exploit di vulnerabilità software. Una compromissione può portare alla perdita di dati, alla violazione della privacy, al furto di informazioni sensibili o al danneggiamento del sistema stesso.

2. Tecniche di contenimento

Le attività di contenimento hanno lo scopo primario di isolare l'incidente in modo tale che non possa creare ulteriori danni a reti/sistemi.

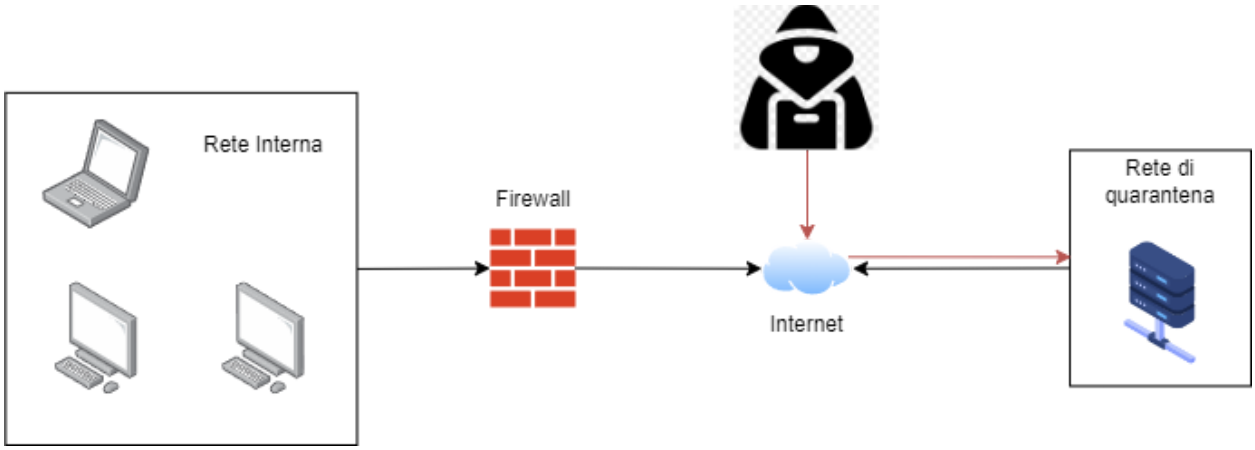
2.1 Segmentazione

Una delle tecniche preventive e strategiche per la gestione degli incidenti di sicurezza sulla rete è la segmentazione, che risulta essere particolarmente utile anche nella fase di **contenimento** di un incidente in corso. La segmentazione include tutte quelle attività che permettono di dividere una rete in diverse LAN o VLAN, separando così il sistema infetto dagli altri, creando una rete ad hoc chiamata rete di quarantena.



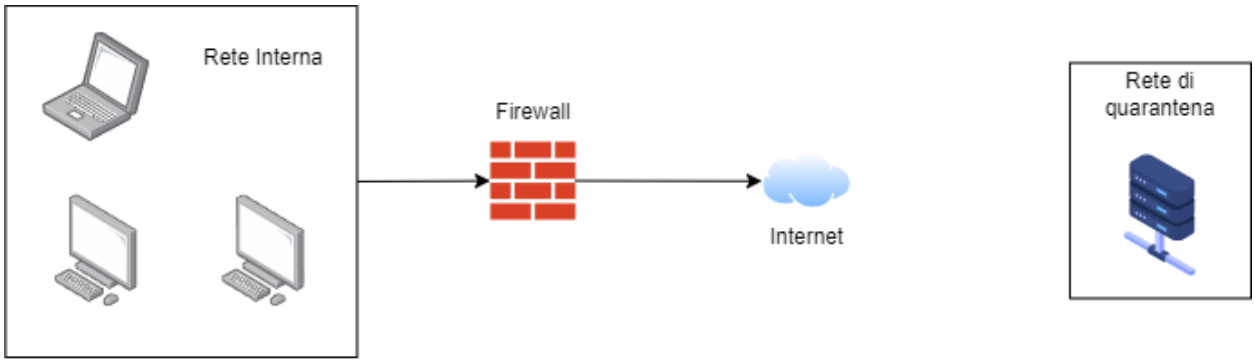
2.2 Isolamento

Quando la segmentazione della rete non è sufficiente e si necessità di un contenimento maggiore, si utilizza la tecnica dell'isolamento, mostrato nella figura di seguito. L'isolamento consiste nella completa disconnessione del sistema infetto dalla rete, per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante. Notate che in questo scenario l'attaccante ha ancora accesso al sistema C tramite internet



2.3 Rimozione

Ci sono casi in cui l'isolamento non è ancora abbastanza, si procede con la tecnica di contenimento più stringente, ovvero la completa rimozione del sistema dalla rete sia interna sia internet. In quest'ultimo scenario, l'attaccante non avrà né accesso alla rete interna né tantomeno alla macchina infettata.



3. Eliminazione informazioni sensibili

Clear: cancellare i dati da un disco rigido significa sovrascrivere più e più volte i dati esistenti con valori casuali o nulli, rendendo così i dati originali meno accessibili o recuperabili. Questo metodo non elimina completamente i dati dal disco, ma li rende molto difficili da recuperare usando strumenti standard di recupero dati. Tuttavia, è ancora possibile recuperare i dati con strumenti specializzati o tramite analisi forense avanzata.

Purge: la pulizia dei dati va oltre la semplice cancellazione. Questo processo coinvolge spesso l'utilizzo di algoritmi di sovrascrittura più sofisticati e ripetuti, che rendono i dati originari praticamente irrecuperabili. La pulizia dei dati può essere implementata attraverso strumenti software specializzati o tramite procedure hardware che implicano l'utilizzo di forti magneti.

Destroy: distruggere i dati implica la completa eliminazione fisica del supporto di memorizzazione, rendendo impossibile il recupero dei dati. Questo può essere fatto distruggendo fisicamente il disco rigido, ad esempio attraverso trituratori o dischi abrasivi, oppure fondendolo o incenerendolo. Questo metodo è estremamente sicuro ma può essere costoso e non sempre pratico, specialmente per grandi quantità di dati o per dispositivi che devono essere riciclati o riutilizzati.