EPICODE-CS0124
S9/L4 - Pratica

Flaviano Sedici

Indice

Riferimenti e versioni

Responsabile del documento: Flaviano Sedici

Versionamento

Versione	Descrizione	Riferimento	Data
1.0	Redazione documento	Responsabile	21/03/2024

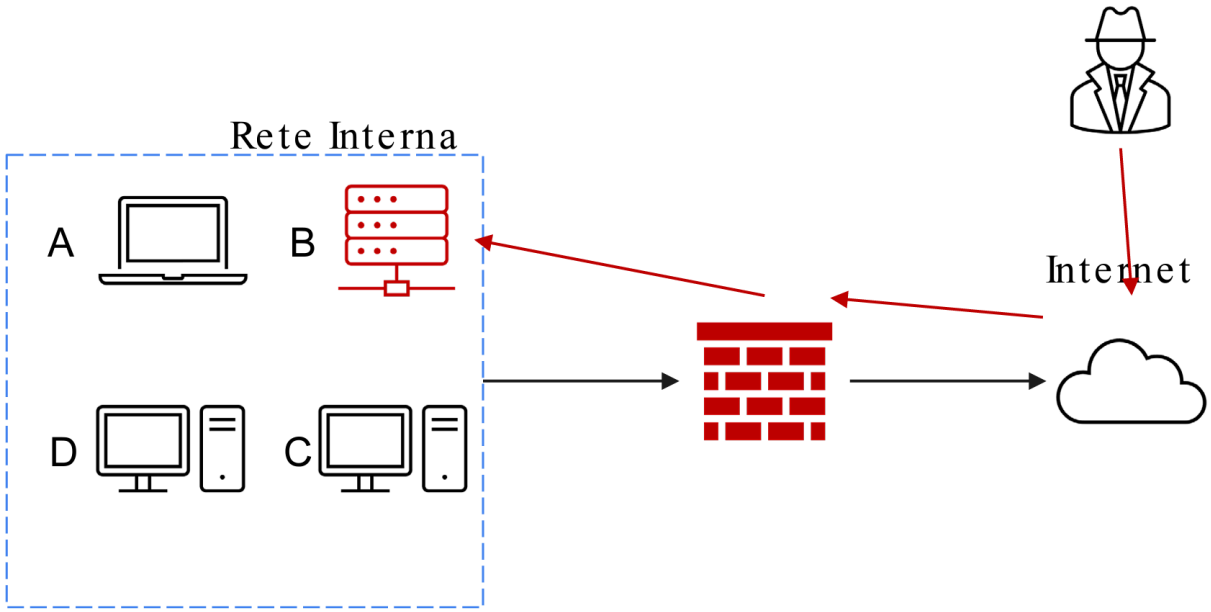
1. Traccia

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: 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**.



Rete iniziale

1.1. Definizioni

Prima di iniziare le scansioni richieste, definiamo il contesto operativo e gli strumenti utilizzati.

1.1.1. Definizioni

Incident Response

L'incident response, o risposta agli incidenti, è il processo di gestione e mitigazione di eventi di sicurezza informatica o violazioni della sicurezza. Coinvolge l'identificazione, la valutazione e la risposta a incidenti di sicurezza, al fine di ripristinare la sicurezza e la continuità operativa di un sistema o di un'organizzazione. Le attività di risposta agli incidenti includono la raccolta di informazioni sull'incidente, l'analisi delle cause, la mitigazione dei danni, la risoluzione del problema e la documentazione delle lezioni apprese per migliorare le misure di sicurezza future. L'obiettivo principale della risposta agli incidenti è di ridurre al minimo l'impatto di un incidente sulla sicurezza e ripristinare rapidamente le operazioni normali.

CSIRT

CSIRT, acronimo di Computer Security Incident Response Team, è un team specializzato nella gestione degli incidenti di sicurezza informatica. I CSIRT sono responsabili della rilevazione, dell'analisi e della risposta agli eventi di sicurezza informatica, al fine di proteggere i sistemi e le risorse dell'organizzazione da minacce e violazioni della sicurezza. Questi team sono composti da esperti di sicurezza informatica e possono essere interni all'organizzazione o esterni, come servizi forniti da terze parti o da enti governativi. I CSIRT svolgono un ruolo cruciale nella gestione della sicurezza informatica, garantendo una risposta efficace agli incidenti e contribuendo a mantenere la sicurezza e l'integrità delle risorse informatiche.

1.2. Incident Response

1.2.1. Analisi e isolamento

Rilevata la presenza di un attacco sul server B, viene messa in atto la procedura di Incident Response procedendo immediatamente all’isolamento dell’asset dalla rete in modo che l’attaccante non possa continuare ad infiltrarsi in altri asset nella rete interna.

L’isolamento può avvenire in tre modi commisurati alla pericolosità della minaccia:

Quarantena - il server B viene isolato in una VLAN dedicata e separata dalla rete interna.

Isolamento - il server B viene collegato direttamente ad internet in modo che sia al di fuori di qualunque rete interna e del firewall, impedendo qualunque tipo di ulteriore contaminazione eventuale della rete o del firewall stesso.

Rimozione - il server B viene isolato totalmente e analizzato on-site in modo da interrompere qualsiasi collegamento con l’attaccante e con la rete interna ed esterna. Questo caso estremo è molto utile nel momento in cui ci siano informazioni estremamente sensibili per l’impresa.

1.2.2. Rimozione della minaccia

Una volta isolato il server, si procedere all’eliminazione della minaccia tramite le seguenti metodologie:

Clear - al fine di ripulire completamente il database infetto si procede con un approccio logico, ovvero la sovrascrittura ripetuta più volte dei dispositivi di storage.

Purge - dopo aver applicato la metodologia Clear, la sicurezza sulla corretta risoluzione della minaccia può essere incrementata tramite metodi fisici come potenti magneti che rendono inutilizzabile i dispositivi magnetici come hard disk.

Destroy - infine è possibile procedere alla completa distruzione del dispositivo tramite la polverizzazione o l'esposizione a temperature elevate che comportino la completa distruzione dell'asset.

Da questo si desume che i metodi di rimozione della minaccia sono sequenziali e incrementali tra loro.