ESERCITAZIONE WEEK 20 DAY1

EPICODE

W20D1 - Pratica (1) PDF

Esercizio
Incident response

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.

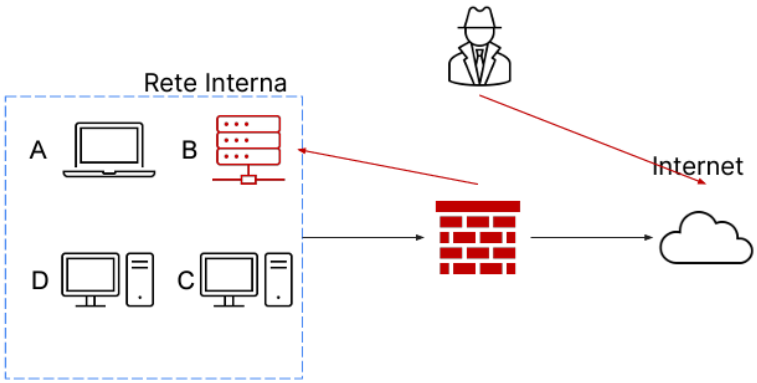
L'attacco è attualmente in corso e siete parte del team di CSIRT.

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**

EPICODE

Esercizio
Incident response



Isolamento

L'isolamento consiste nella completa disconnessione del sistema infetto dalla rete, per restringere ancora maggiormente l'accesso alla rete interna da parte dell'attaccante, rispetto alla semplice segmentazione.

Quindi in questo caso il sistema B, verrà non solo messo in una rete di quarantena per separarlo dai sistemi A, C e D, ma verrà disconesso dalla rete interna, senza condividere nemmeno il firewall con i dispositivi. Rimane però comunque la possibilità di avere accesso a internet.

Rimozione

Ci sono casi in cui l'isolamento non è ancora abbastanza. In questi casi si procede con la tecnica di contenimento più stringente, ovvero la completa rimozione del sistema B dalla rete sia interna sia internet. Quindi l'attaccante non avrà né accesso alla rete interna né tantomeno al database in questione.

Per l'eliminazione delle informazioni sensibili, prima di procedere allo smaltimento dei dischi compromessi, si può procedere con diverse tecniche:

Clear: i dischi vengono completamente ripuliti dal loro 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 i dispositivi 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 sui dischi;

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.