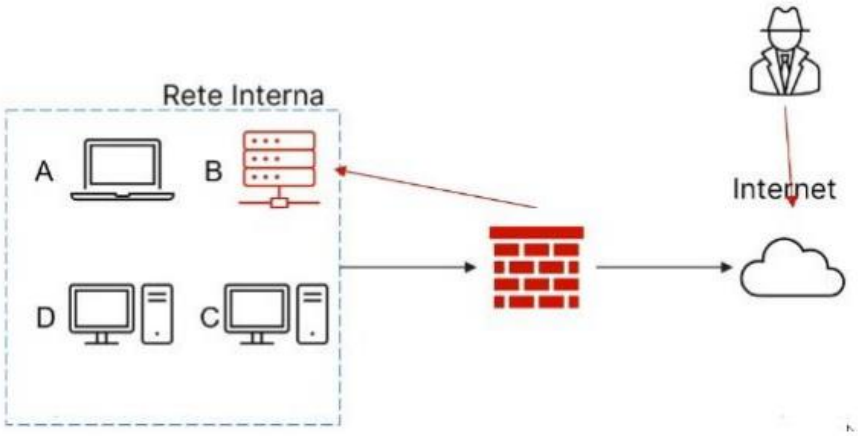
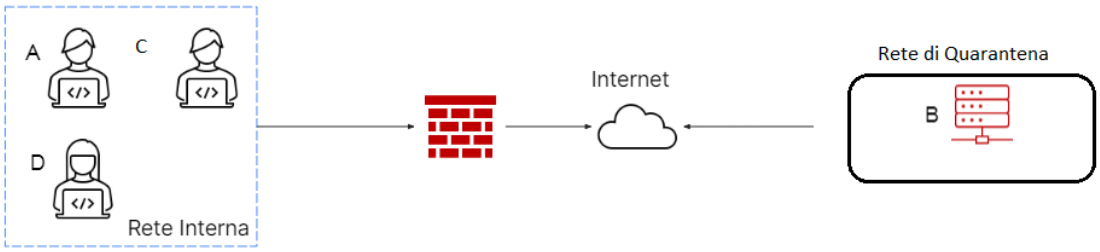
Epicode Unit 3 Day 4

Incident Response

Nella simulazione odierna, viene richiesto allo studente di illustrare i vari step necessari per l'implementazione di una corretta risposta ad un eventuale incidente su un asset. Nel caso specifico, l'attacco va a segno attraverso un canale Web, per andare ad "infettare" il Server B in figura:

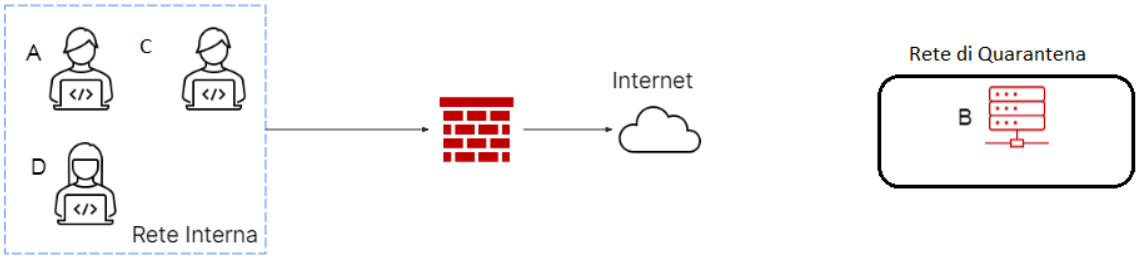


Come si può notare, il server si trova sula rete interna e collegato pertanto ad altre macchine, motivo per cui la prima azione da eseguire sarà quella dell' Isolamento, ovvero la rimozione della macchina infetta dalla suddetta rete interna per evitare che possibili worm, o altri tipi di codice malevolo, possano raggiungere il resto dell'infrastruttura. Si noti che in tale configurazione l'asset bersaglio risulta ancora connesso ad internet, lasciando pertanto ancora un minimo di libertà d'azione all'attaccante, pur non potendo questi "allargare" il suo raggio d'azione.



Nonostante quanto affermato, questa tecnica risulta essere spesso utilizzata dai CSIRT per proseguire con la raccolta di informazioni sulla natura e l'origine dell'attacco, utilizzando quindi il bersaglio come fosse una sorta di "esca".

Un altro metodo di risposta potenzialmente efficace è quello della RIMOZIONE, attraverso il quale la macchina attaccata viene completamente isolata per evitare che l'attacco procuri ulteriori danni al target. Di seguito una rappresentazione grafica della tecnica di Rimozione.



Una volta fatto ciò, sarà compito del CSIRT procedere all'eliminazione di dati sensibili potenzialmente compromessi una volta conclusa la fase di risposta ed effettuato il regolare ripristino dei sistemi.

Tali azioni avvengono generalmente mediante l'utilizzo delle tecniche di PURGE, DESTROY, CLEAR. Analizzando nel dettaglio:

PURGE:

Con "Purge" si intende la rimozione di dati sensibili mediante metodi logici o fisici quali la smagnetizzazione, generalmente tramite degausser, che rende i dati inaccessibili a sistemi, macchine e lettori specifici. In questo modo si ha la sicurezza di impossibilità di recupero fisico dei medesimi dati da parte di utenti o figure non autorizzate.

DESTROY:

La tecnica di "Destroy" rilsulta essere più drastica ed economicamente dispendiosa della precedente. I dati vengono fisicamente annichiliti con tecniche

di laboratorio quali la disintegrazione, la foratura dei dischi o la polverizzazione. Questi metodi, come già detto decisamente più drastici, rendono i dati inaccessibili a chiunque.

CLEAR:

Con "Clear" si intende l'esecuzione di tecniche logico-informatiche per la pulizia dei dischi compromessi. Una delle più comuni è senza dubbio quella della sovrascrittura ripetuta che va a "ripulire" il sistema di archiviazione attaccato (metodo del "red-and-write"). Fa inoltre parte dei metodi "Clear" il factoy-reset della macchina (formattazione) che seppur garantendo una totale pulizia della stessa, viene generalmente utilizzato come "last resource" in quanto a valle di quest'ultimo sarebbe necessaria la ri-configurazione dell'intero sistema attaccato.