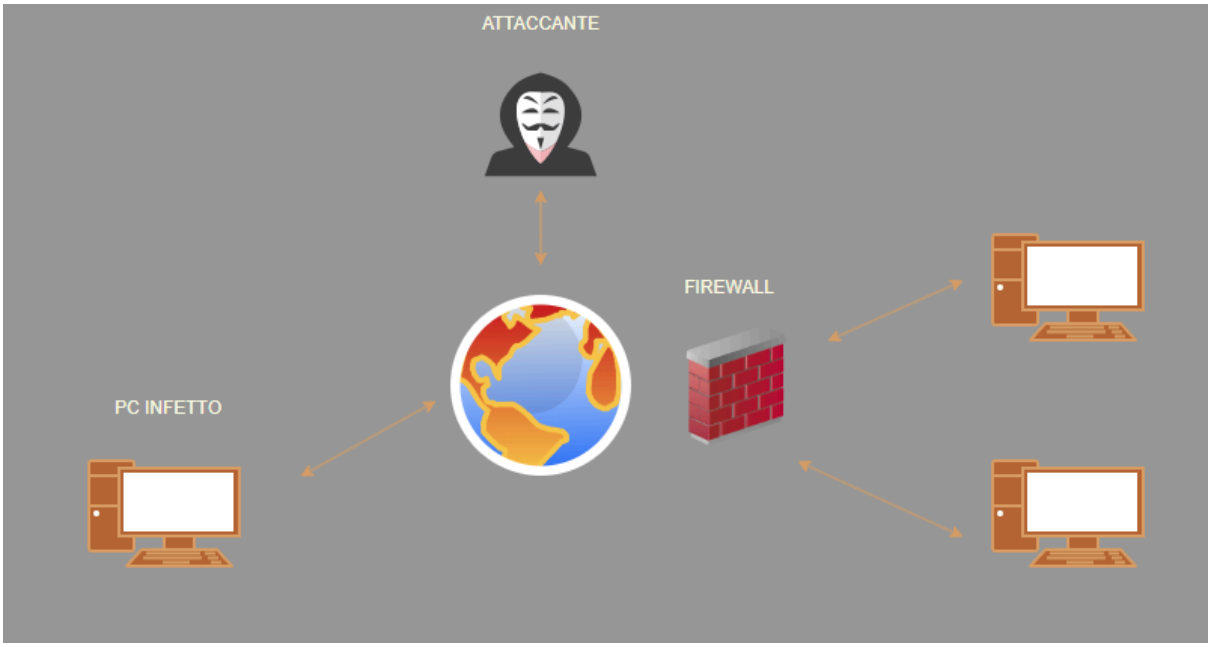
S9/L4

L’esercizio di oggi prevede di isolare un computer infetto da una LAN in modo da ridurre il rischio di trasmettere il virus agli altri dispositivi.

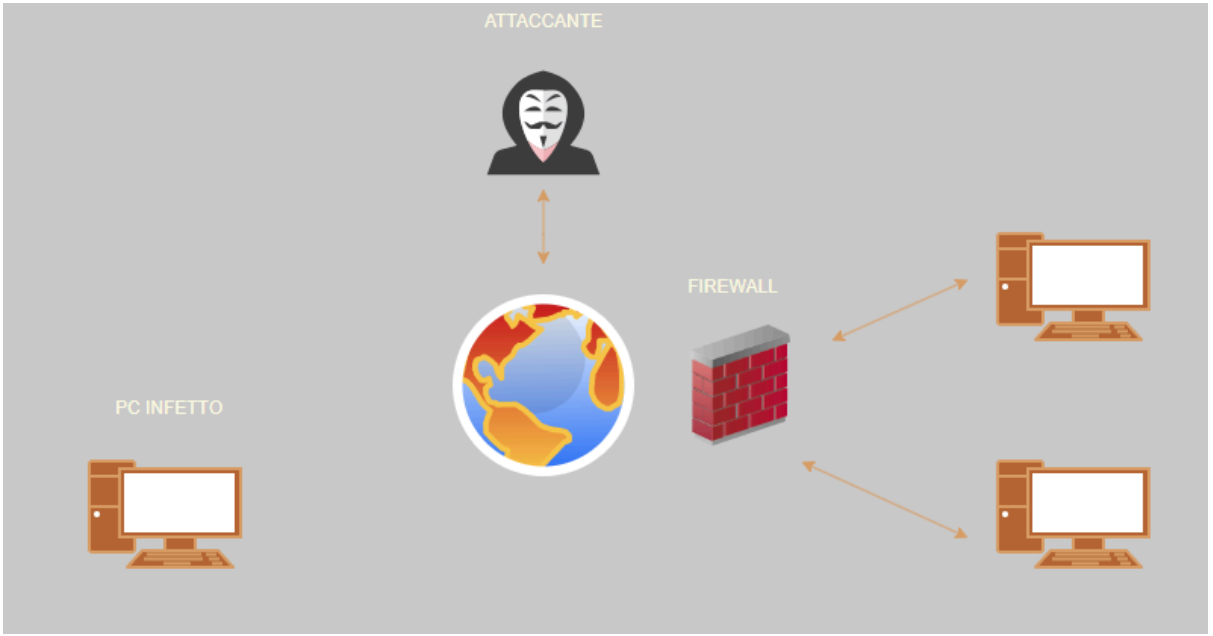
Traccia: Con riferimento alla figura in slide 4, il sistema B (un database con diversi dischi per lo storage) è stato compromesso interamente da un attaccante che è riuscito a bucare la rete ed accedere al sistema tramite Internet. L’attacco è attualmente in corso e siete parte del team di CSIRT. Rispondere 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.

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.

Come si vede nell'immagine abbiamo isolato il PC infetto dal suo ambiente con gli altri pc.



Per avere una maggiore sicurezza andiamo ad **ISOLARE** levandogli anche l'accesso ad Internet. In questo caso l'attaccante non avrà né più accesso alla rete interna né ad internet.



Certamente! Eccole suddivise senza essere elencate:

A valle delle attività di contenimento, il team CSIRT deve passare alla fase di rimozione dell'incidente. In questa fase lo scopo è eliminare tutte le attività, le componenti, i processi che restano dell'incidente all'interno della rete o sui sistemi. Questa attività può includere, ad esempio, la rimozione di eventuali backdoor installate da un malware, oppure ripulire dischi e chiavette USB compromesse. La fase di rimozione dipende molto da che tipo di incidente di sicurezza è in corso. Una lista dettagliata delle attività da seguire per macro-casistica deve essere elencata nei **"playbooks".**

La fase di recupero consiste nel ristabilire la normale operatività delle applicazioni e dei servizi. Include ad esempio **il recupero dei dati** e delle informazioni perse, **l'applicazione delle patch dove disponibili** per eventuali sistemi obsoleti, l**a revisione delle politiche dei firewall**, **IPS e IDS oppure l'aggiornamento delle firme degli antivirus**.

Dopo l'attacco , server e hosts non sono più considerati sicuri , di conseguenza saranno ripuliti con le seguenti tecniche:

Reconstruction: include tutte quelle attività che mirano a recuperare quelle parti ancora affidabili di un sistema compromesso.
Rebuilding: include tutte quelle attività che mirano a ricostruire interamente un sistema impattato considerato non più affidabile.

FASE DI SMALTIMENTO O RIUTILIZZO

Purge: si adotta non solo un approccio logico per la rimozione dei contenuti sensibili 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.

Il metodo Destroy è più efficace ma molto più costoso; la decisione dipende dal budget disponibile dell'azienda

Il metodo **CLEAR** fa parte anch’esso della fase del riutilizzo ed è il più economico perchè 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. Non vengono utilizzati metodi fisici.