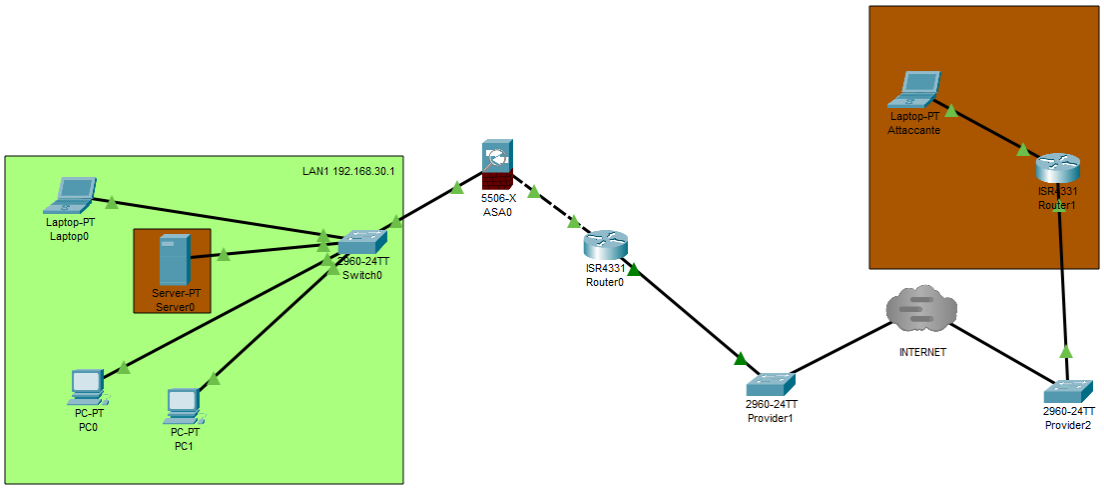
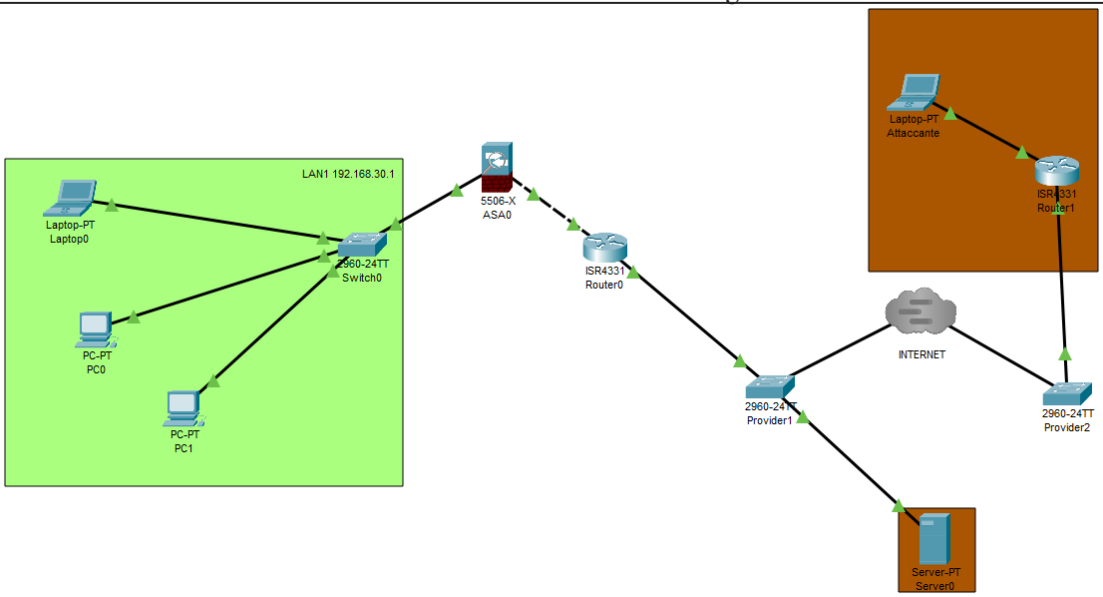
Incident Response

03-23-2023

L'immagine sotto riportata fa vedere come un attaccante sia riuscito tramite internet a violare la nostra rete infettando un database situato nella nostra rete interna.



Quindi per evitare qualsiasi complicazione e la possibile proliferazione nel sistema da parte di un utente malintenzionato procediamo con la completa disconnessione dalla rete interna dell'azienda lasciando il database direttamente connesso ad internet.
L'isolamento nella rete di quarantena ci permette di non notificare l'attaccante delle nostre azioni ma al contempo lo limitiamo al singolo database, quindi si può procedere con la disconnessione tramite cavo dalla rete e la seguente rimozione del malware o la distruzione dell'hardware, ma prima di passare a questo, dato che sia noi che l'attaccante abbiamo accesso alla macchina tramite internet possiamo tentare di attuare azioni di tracciamento del malintenzionato con le conseguenze del caso.



Una volta effettuata la disconnessione totale della macchina possiamo abbiamo a disposizione tre scelte, la prima chiamata clear punta a riportare il componente allo stato di fabbrica usando varie sovrascrizioni (dalle 3 alle 7) oppure se disponibile si utilizza la funzione factory reset, una tecnica più aggressiva è quella del purge che cosiste in un clean con l'aggiunta di una rimozione fisica tramite forti magneti dei contenuti ritenuti sensibili o inaffidabili, l'ultima e quella del destroy che come suggerisce il nome implica da distruzione completa dell'hardware senza la possibilità di recuperare alcun dato, quest'ultima avviene solo in casi estremi ed implica un dispendio di tempo e soldi superiore alle altre.

POST-INCIDENT

Per far si che una situazione del genere non capiti più si può pensare di aggiungere ulteriori sistemi di sicurezza sulla rete o se il problema è scaturito da una negligenza da parte di un dipendente, dei corsi formativi che sensibilizzino sulle principali fonti di pericolo e diano i mezzi per evitarle sarebbero d'obbligo.