COMMENTO SULLE AZIONI DI MITIGAZIONE ADOTTATE NULL SESSION E ARP POISONING

NULL SESSION: nel laboratotrio svolto l'attenzione è stata posta sul comprendere il funzionamento della vulnerabilità e sulle possibili azioni di mitigazione da adottare per evitarne lo sfruttamento.
La NULL Session sfrutta una configurazione debole del servizio SMB che consente connessioni anonime, permettendo a un attaccante di enumerare utenti, gruppi e condivisioni di rete senza fornire credenziali valide.
Nel contesto dell'esercizio, la mitigazione di questa vulnerabilità consiste nel disabilitare l'accesso anonimo ai servizi SMB e nel limitare l'enumerazione delle informazioni di rete ai soli utenti autenticati. In questo modo viene eliminata la possibilità di stabilire sessioni anonime, che rappresentano il presupposto dell'attacco.
L'efficacia di questa mitigazione è elevata, poiché impedisce direttamente lo sfruttamento della NULL Session: senza accesso anonimo, l'attaccante non può raccogliere informazioni sensibili sul sistema.
Dal punto di vista dell'utente finale, l'impatto è minimo o nullo, in quanto l'accesso alle risorse di rete avviene normalmente tramite autenticazione.
Per l'azienda, l'effort richiesto è basso, poiché la mitigazione può essere applicata tramite configurazioni di sicurezza del sistema operativo e policy di rete, senza richiedere modifiche infrastrutturali complesse.

ARP POISONING: per quanto riguarda l'ARP Poisoning, l'esercizio ha mostrato come questa tecnica di attacco sfrutti il funzionamento del protocollo ARP, che non prevede meccanismi di autenticazione per la risoluzione degli indirizzi IP in indirizzi MAC all'interno di una rete locale.
Questa caratteristica consente a un attaccante di inviare messaggi ARP falsificati, alterando le associazioni IP–MAC presenti nella rete e posizionandosi come intermediario nella comunicazione tra due host legittimi.
Nel contesto dell'attività svolta, la mitigazione dell'ARP Poisoning si basa principalmente sull'adozione di misure di prevenzione e controllo a livello di rete; in particolare, l'utilizzo di funzionalità di sicurezza sugli switch gestiti, come il controllo delle risposte ARP, e la segmentazione della rete permettono di ridurre la possibilità che un attaccante possa introdurre associazioni IP–MAC false all'interno del dominio di broadcast.
Un ulteriore aspetto emerso durante l'esercizio riguarda l'importanza della protezione del traffico applicativo.

VALUTAZIONE COMPLESSIVA

L'attività svolta ha permesso di comprendere in modo pratico come vulnerabilità di natura diversa, a livello di servizio e a livello di rete, possano compromettere la sicurezza di un sistema informatico.

Nel caso della NULL Session, è emerso come una configurazione debole dei servizi SMB possa consentire l'accesso non autorizzato a informazioni sensibili, mentre nel caso dell'ARP Poisoning è stato possibile osservare come l'assenza di meccanismi di autenticazione nel protocollo ARP renda possibile l'intercettazione del traffico di rete.

Le azioni di mitigazione analizzate risultano coerenti con le vulnerabilità osservate e affrontano direttamente le cause che rendono possibile lo sfruttamento degli attacchi.

La disabilitazione dell'accesso anonimo ai servizi SMB elimina il presupposto della NULL Session, mentre le contromisure di rete e l'utilizzo di protocolli cifrati riducono in modo significativo l'impatto di un attacco di tipo Man-In-The-Middle basato su ARP Poisoning.

Dal punto di vista operativo, le mitigazioni proposte non comportano un impatto rilevante sull'utente finale, che continua a utilizzare i servizi senza variazioni percepibili.

L'effort richiesto è invece maggiore per l'ARP Poisoning, poiché richiede una gestione più attenta dell'infrastruttura di rete, ma risulta giustificato dalla maggiore protezione dei dati trasmessi.

Nel complesso, l'esercizio evidenzia l'importanza di una corretta configurazione dei servizi di rete e dell'adozione di adeguate misure di sicurezza, mostrando come anche sistemi apparentemente funzionanti possano risultare vulnerabili in assenza di controlli specifici.