Esercizio Null Session Daniele Atzori
M4-W15-D1

Una "null session" su Windows è un tipo di connessione anonima che non richiede autenticazione. Questo tipo di connessione sfrutta una vulnerabilità nei servizi di condivisione di file e stampanti, permettendo a un utente non autenticato di ottenere informazioni sensibili sul sistema, come gli elenchi degli utenti, dei gruppi e delle condivisioni di rete. Le null session utilizzano il protocollo SMB (Server Message Block) e possono essere stabilite su porte come la 139 (NetBIOS) e la 445 (SMB diretto).

Una soluzione rapida sarebbe disabilitare completamente la condivisione file per tutti i computer della rete aziendale ma questo comporterebbe dei problemi di praticità rendendo il lavoro di tutti i giorni più complicato.

Per mitigare il problema delle null session su Windows, è necessario implementare alcune configurazioni di sicurezza. Prima di tutto, è consigliabile disabilitare le connessioni anonime. Per farlo, bisogna aprire l'Editor dei criteri di gruppo locali (gpedit.msc), navigare in Configurazione computer → Impostazioni di Windows → Impostazioni di sicurezza → Criteri locali → Opzioni di sicurezza, e configurare il criterio "Restrict anonymous access to named pipes and shares" impostando "Restrict anonymous access to Named Pipes and Shares". Inoltre, è importante configurare il criterio "Let everyone permissions apply to anonymous users" impostandolo su "Disabled".

Configurare le autorizzazioni di condivisione dei file solo per gli utenti che ne abbiano una reale necessità, al fine di evitare che troppi utenti abbiano privilegi di visualizzazione-modifica-condivisione di file sensibili.

Configurare il firewall per bloccare le porte 139 e 445, a meno che non siano strettamente necessarie per la rete, è un'altra misura di sicurezza essenziale. È importante assicurarsi che il firewall sia configurato per bloccare il traffico SMB da e verso la rete pubblica.

Tenere il sistema operativo Windows e tutti i software aggiornati con le ultime patch di sicurezza è cruciale. Implementare il monitoraggio e il logging delle connessioni SMB aiuta a rilevare eventuali tentativi di null session. Utilizzare strumenti di sicurezza per verificare periodicamente la configurazione del sistema e identificare potenziali vulnerabilità è un'ulteriore misura di sicurezza.

La gestione delle null session è fondamentale per la sicurezza delle reti Windows. Implementando le configurazioni e le pratiche di cui sopra, si può ridurre significativamente il rischio associato a questo tipo di connessioni non autorizzate.