

Null Session

Una delle vulnerabilità storiche windows sono le Null Session.

La Null Session si usa per recuperare informazioni come :

Password

Utenti di un sistema

Processi in esecuzione

Programmi aperti

Le Null Session si possono utilizzare da remoto e senza autenticazione.

Questi attacchi si basano su una vulnerabilità dell'autenticazione delle share amministrativi Windows.

Negli anni scorsi, la maggior parte dei sistemi Windows era vulnerabile alle Null Session, e

gli attacchi di questo tipo hanno avuto un impatto enorme su tutti i sistemi Windows.

Ad oggi sono molto pochi i sistemi vulnerabili.

Per mitigare le null session ci sono diverse azioni da effettuare, con valutazione dell'efficacia e dell'effort richiesto sia per gli utenti, che per l'azienda.

- 1) La soluzione più efficace per mitigare le Null Session è disabilitarle completamente. Può essere fatto modificando le impostazioni di sicurezza del sistema operativo Windows. L'utente può farlo facilmente, ma l'azienda dovrebbe pianificare attentamente l'implementazione su tutti i sistemi interessati.
- 2) Microsoft ha rilasciato patch di sicurezza per affrontare le vulnerabilità Null Session in diverse versioni di

Windows. Gli utenti dovrebbero assicurarsi di mantenere aggiornato il loro sistema operativo con le ultime patch di sicurezza. Tuttavia l'azienda deve pianificare e gestire il processo di applicazione delle patch su tutti i sistemi, il che può richiedere più tempo e risorse.

- 3) Monitorare e gestire il traffico di rete e i tentativi di accesso non autorizzato può aiutare a rilevare e rispondere tempestivamente agli attacchi Null Session. Gli utenti non sono direttamente coinvolti, ma l'azienda deve configurare e gestire un sistema di monitoraggio e login efficace.

In generale, una combinazione di queste azioni di mitigazione è spesso la miglior strategia per affrontare il problema delle

Null Session. Mentre alcune misure possono essere implementate dagli utenti stessi, altre richiedono un impegno maggiore da parte dell'azienda.