Una "NULL session" si verifica quando si accede a un sistema senza nome utente o password, quindi un attaccante riesce a collegarsi ad una share remota o locale senza auentificazione. Questa connessione permette a un utente o a un'applicazione di accedere a determinate informazioni di sistema o risorse senza richiedere un'autenticazione formale, nome utente e password. Tuttavia, a causa della mancanza di autenticazione, le NULL session possono rappresentare una vulnerabilità di sicurezza, poiché possono essere sfruttate da attaccanti per raccogliere informazioni sensibili o eseguire azioni non autorizzate.

I sistemi vulnerabili a NULL session includono principalmente i sistemi operativi Windows, in particolare quelli basati sulla famiglia di sistemi operativi Windows NT (ad esempio, Windows NT, 2000, XP, 7, ecc.).

Ecco alcune modalità per risolvere le vulnerabilità legate alle NULL session:

1. Disabilitare le NULL session: La soluzione più diretta è disabilitare completamente le NULL session sul sistema operativo Windows. Questo può essere fatto modificando la configurazione del Registro di sistema o tramite le impostazioni di gruppo. Questa soluzione è semplice da effettuare e non richiede un investimento economico all'azienda, consentendo quindi di applicare una rapida soluzione al problema.

2. Aggiornare il sistema operativo: Mantenere il sistema operativo aggiornato con le ultime patch di sicurezza è fondamentale. Anche questa soluzione è di facile applicazione e non richiede particolari investimenti economici all'azienda , si tratta quindi solo di prestarvi attenzione. (questa soluzione potrebbe non essere la più economica se nell'azienda ci sono macchine vecchie che non permettono più l'aggiornamento.)

3. Impostare le autorizzazioni in modo appropriato: Verificare che le autorizzazioni per le risorse di rete siano configurate correttamente. Questo include definire chi può accedere a quali risorse e limitare l'accesso anonimo alle risorse sensibili. Questa soluzione richiede probabilmente l'intervento di un tecnico ed è quindi è meno immediata oltre al fatto che richiede anche se non eccessivo un esborso economico per l'azienda; è tuttavia fondamentale configurare correttamente le autorizzazioni.

4. Utilizzare soluzioni di sicurezza aggiuntive: Considerare l'utilizzo di soluzioni di sicurezza aggiuntive, come firewall, sistemi di rilevamento delle intrusioni (IDS) e sistemi di autenticazione a più fattori (MFA), per aggiungere un ulteriore strato di protezione. Questa soluzione richiede un investimento economico da parte dell'azienda che però la renderebbe molto meno vulnerabile a questo ma anche ad altri tipi di attacco migliorandone sensibilmente la sicurezza informatica.

5. Monitorare e registrare l'accesso: Implementare sistemi di monitoraggio e registrazione per rilevare e registrare attività sospette, inclusi tentativi di accesso NULL session non autorizzati. Questa soluzione come per il punto 4 richiede si un investimento economico che però renderebbe l'azienda meno vulnerabile non solo per questo tipo di minaccia.

6. Assicurarsi che gli utenti e gli amministratori del sistema siano consapevoli delle minacce legate alle NULL session e delle migliori pratiche per prevenirle. Questa piuttosto che una vera e propria soluzione è un'azione di prevenzione, infatti investire in corsi di aggiornamento sulla sicurezza informatica per i dipendenti potrebbe costare meno di quanto costerebbe poi risolvere un eventuale minaccia.

È importante notare che molti dei sistemi operativi Windows più recenti hanno implementato misure di sicurezza migliorate per mitigare le NULL session, quindi è fondamentale mantenere il sistema operativo aggiornato per beneficiare di queste migliorie.