Null Session

Le Null Session sono connessioni di rete anonime e non autenticate ad una macchina Windows che consentono ad un utente di accedere ad informazioni di sistema senza dover inserire alcune credenziali di accesso. Questa vulnerabilità è stata sfruttata parecchio in passato per ottenere informazioni sensibili e compiere attacchi di tipo ‘enumeration’ su reti Windows.

I sistemi operativi Windows NT, 2000, XP e 2003 erano particolari vulnerabili alle Null Session. Tuttavia, a partire da Windows Vista e versioni successive, Microsoft ha apportato modifiche significative per mitigare questa vulnerabilità, rendendo più difficile l’accesso anonimo alle informazioni di sistema.

Per risolvere questa vulnerabilità e mitigare i rischi associati alle Null Session , è consigliabile adottare le seguenti misure:

1) Aggiornare il sistema operativo: Assicurarsi di utilizzare la versione più recente del sistema operativo Windows, che includa le correzioni di sicurezza e le migliorie introdotte da Microsoft per mitigare le Null Session.

2) Disabilitare le connessioni Null Session: Verificare che le connessioni Null Session siano disabilitate nel registro di sistema. Modificare le impostazioni di registro appropriate per impedire l'accesso anonimo alle risorse di sistema.

3) Applicare correttamente i permessi di condivisione: Impostare i permessi di condivisione delle risorse di rete in

modo adeguato, garantendo che solo gli utenti autorizzati abbiano accesso ai dati sensibili.

4) Utilizzare firewall e filtri di rete: Configurare un firewall o un dispositivo di filtraggio di rete per bloccare o limitare le connessioni in ingresso dalle connessioni Null Session.

5) Monitoraggio del traffico di rete: Implementare una soluzione di monitoraggio del traffico di rete per rilevare eventuali tentativi di connessione Null Session o attività anomale.

L'efficacia di queste misure dipende dal corretto implementazione e configurazione del sistema operativo e delle misure di sicurezza. Anche se le versioni più recenti di Windows hanno ridotto notevolmente la vulnerabilità alle Null Session, è importante mantenere il sistema operativo aggiornato e adottare un approccio di sicurezza olistico che includa anche altre misure di protezione della rete e dei dati.