NULL SESSION

Una "Null Session" è una connessione non autenticata a un sistema, generalmente un server Windows, utilizzando credenziali vuote o inesistenti. Questo tipo di connessione sfrutta una vulnerabilità nei protocolli di condivisione delle risorse, come SMB (Server Message Block), permettendo a un utente non autenticato di ottenere accesso a determinate informazioni di sistema, come condivisioni di rete, liste di utenti e gruppi, e altre risorse.
Le Null Session erano una vulnerabilità particolarmente rilevante nelle versioni più vecchie dei sistemi operativi Windows, dove potevano essere utilizzate per raccogliere informazioni utili per attacchi successivi.

I principali sistemi vulnerabili a questo tipo di attacco includono:
- Windows NT 4.0
- Windows 2000
- Windows XP (prima del Service Pack 2)
- Windows Server 2003 (prima del Service Pack 1)

Tuttavia, le versioni più recenti di Windows hanno implementato misure di sicurezza per mitigare questi rischi, rendendo le Null Session molto meno rilevanti.

Per mitigare o risolvere la vulnerabilità delle **Null Session** su sistemi operativi vulnerabili, esistono diverse misure di sicurezza che possono essere adottate, come:

- **Aggiornamenti e Patch:** Installare gli ultimi Service Pack e aggiornamenti di sicurezza forniti da Microsoft. Ad esempio, aggiornare Windows XP a Service Pack 2 o superiore, e Windows Server 2003 a Service Pack 1 o superiore.Windows 2000
- **Migrazione a Sistemi Moderni:** Aggiornare a versioni più recenti di Windows, come Windows 10, Windows 11, o versioni più moderne di Windows Server, che hanno integrato miglioramenti di sicurezza.Windows Server 2003 (prima del Service Pack 1)
- **Criteri di Sicurezza di Gruppo (Group Policy):** Configurare i criteri di sicurezza per bloccare le connessioni anonime impostando policy di rete
- **Protezione delle Condivisioni di Rete:** Impostare autorizzazioni su condivisioni e cartelle in modo che solo gli utenti autenticati possano accedervi.
- **Rimozione di Condivisioni Anonime:** Eliminare o ridurre al minimo le condivisioni di rete che consentono accessi anonimi.
- **Firewall:** Configurare il firewall per bloccare il traffico SMB sulla rete da fonti non attendibili o sconosciute.
- **IDS/IPS:** Implementare sistemi di rilevamento e prevenzione delle intrusioni che possono monitorare e bloccare tentativi di connessioni anonime sospette.
- **Audit e Logging:** Monitorare e registrare le attività di rete, prestando particolare attenzione ai tentativi di connessione anonima. Questo può aiutare a rilevare e rispondere tempestivamente a potenziali attacchi.