# Null session

Una null session è una connessione anonima non autorizzata a un sistema operativo Windows tramite la rete. Si tratta di un accesso senza credenziali o autenticazione, che permette a un potenziale aggressore di interrogare il sistema e recuperare informazioni riservate senza aver effettuato l'accesso legittimo.

I sistemi operativi Windows più vecchi, come Windows NT, Windows 2000 e Windows XP, sono particolarmente vulnerabili alle null session. Questo perché di default consentono connessioni anonime che permettono di accedere a informazioni di rete sensibili, come l'elenco degli utenti, le condivisioni di file e i nomi dei computer.

Tuttavia, a partire da Windows Server 2003 e Windows XP SP2, Microsoft ha apportato delle modifiche per mitigare questa vulnerabilità. Le azioni di mitigazione che si possono adottare includono:

1. Disabilitare le connessioni anonime: È possibile configurare il sistema operativo per impedire le connessioni anonime e richiedere l'autenticazione per accedere alle risorse di rete.
2. Applicare correttamente le autorizzazioni di condivisione: Assicurarsi che le condivisioni di file e le risorse di rete siano configurate correttamente, limitando l'accesso solo agli utenti autorizzati e applicando le giuste autorizzazioni di lettura e scrittura.
3. Aggiornare il sistema operativo: Mantenere il sistema operativo Windows e gli altri software installati aggiornati con gli ultimi aggiornamenti di sicurezza. Questo può contribuire a risolvere le vulnerabilità note e ridurre le possibilità di exploit tramite null session.
4. Utilizzare un firewall: Configurare un firewall per bloccare le connessioni in ingresso non autorizzate e filtrare il traffico di rete. Ciò può aiutare a rilevare e prevenire tentativi di accesso tramite null session.
5. Monitoraggio degli accessi: Implementare soluzioni di monitoraggio e rilevamento degli accessi non autorizzati per identificare attività sospette e prendere provvedimenti tempestivi.
6. Educazione e consapevolezza: Fornire formazione e sensibilizzazione agli utenti sulle migliori pratiche di sicurezza informatica, come l'importanza di utilizzare password robuste, evitare l'accesso anonimo e non condividere informazioni sensibili tramite connessioni non sicure.

Seguendo queste azioni di mitigazione, è possibile ridurre significativamente il rischio di exploit attraverso null session e aumentare la sicurezza dei sistemi operativi Windows.