W15D1

Null Session:

La **Null Session** è una sessione che permette di interagire con un sistema Windows senza dover effettuare l'autenticazione.
Questo tipo di connessione sfrutta una vulnerabilità in alcuni protocolli di rete Microsoft, in particolare il protocollo **SMB** (Server Message Block), che consente a un utente remoto di ottenere informazioni dal sistema senza bisogno di credenziali.
Attraverso una Null Session, un attaccante può raccogliere informazioni sensibili come nomi di utenti, gruppi, condivisioni di rete e altre configurazioni del sistema, che possono poi essere utilizzate per ulteriori attacchi.

Sistemi Vulnerabili a Null Session

I sistemi particolarmente vulnerabili a questa problematica sono:

- **Windows NT 4.0**
- **Windows 2000**
- **Windows XP** (fino a un certo punto, a meno che non siano stati applicati aggiornamenti specifici)
- **Windows Server 2003**

Questi sistemi operativi permettevano di stabilire una Null Session di default, ma successivi aggiornamenti di sicurezza hanno cercato di mitigare il problema.

Modalità per Mitigare o Risolvere la Vulnerabilità di Null Session

Per risolvere la vulnerabilità delle *Null Session* e proteggere il tuo sistema da potenziali accessi non autorizzati, puoi seguire alcuni passaggi pratici che miglioreranno la sicurezza del tuo ambiente Windows.

1. Modifica delle Impostazioni nel Registro di Sistema

Una delle prime cose da fare è intervenire sulle impostazioni del registro di sistema. Questo passaggio permette di limitare o disabilitare completamente le connessioni anonime.

2. Configurazione delle Condivisioni di Rete

Configurare le condivisioni di rete per richiedere sempre l'autenticazione e restringere le autorizzazioni agli utenti autenticati.

3. Configurazione del Firewall e delle Regole di Sicurezza

Configurare firewall e altri dispositivi di rete per bloccare il traffico SMB su porte note (come la porta 445) da e verso segmenti di rete non sicuri.

4. Aggiornamento del Sistema Operativo

- Applicare tutte le patch di sicurezza e aggiornamenti forniti da Microsoft per eliminare la possibilità di stabilire Null Session.
- Se si utilizza un sistema operativo obsoleto, è altamente consigliato aggiornare a una versione più recente e supportata.

5. Impostazione di Policy di Gruppo

Implementare Group Policy Objects (GPO) per limitare l'accesso anonimo e configurare impostazioni di sicurezza avanzate per prevenire accessi non autorizzati.

6. Monitoraggio e Logging

Abilitare e monitorare i log di sicurezza per rilevare tentativi di connessioni anonime e rispondere tempestivamente a possibili violazioni della sicurezza.