NULL SESSION

Cosa vuol dire null session

Una null session è una vulnerabilità storica dei sistemi Windows, che consente di connettersi **senza autenticazione** ad un sistema, anche da remoto tramite API o RPC (Remote Procedure Call).

Queste connessioni ad una share locale o remote sono spesso sfruttate per raccogliere informazioni dal sistema di destinazione, come password, utenti e gruppi di un sistema, processi in esecuzione, programmi aperti.

Quali sistemi sono vulnerabili alle null session

Sistemi Windows più vecchi, come Windows NT e alcune versioni di Windows 2000, erano particolarmente vulnerabili alle null sessions. Nel tempo, le versioni successive di Windows hanno introdotto miglioramenti nella sicurezza per mitigare questa vulnerabilità.

Questi sistemi operativi esistono ancora oppure sono estinti da anni e anni?

Windows NT e le prime versioni di Windows 2000 sono ormai considerati obsoleti e non sono più supportati da Microsoft, tuttavia è possibile che alcune istanze di questi sistemi operativi esistano ancora in ambienti legacy (vecchi sistemi, tecnologie, software o hardware che sono ancora in uso, nonostante ci siano sul mercato soluzioni più moderne ed efficienti) o in organizzazioni che non hanno aggiornato i loro sistemi. Tuttavia, la loro presenza è diventata molto rara e la maggior parte delle organizzazioni ha migrato verso sistemi operativi più recenti e sicuri.

Modalità per mitigare o risolvere questa vulnerabilità:

1. **Disabilitare le Null Sessions:** Questo può essere fatto attraverso direttive di gruppo o modificando il registro di sistema.

   Efficacia: Bloccare direttamente l'accesso senza autenticazione è un metodo altamente efficace per prevenire attacchi basati su Null Session.

   Effort: Bassomedio. Richiede una configurazione attraverso direttive di gruppo o modifiche al registro, ma una volta implementato, l'overhead di manutenzione è minimo.

2. **Limitare le connessioni anonime:** Configurare le impostazioni di sicurezza per rifiutare richieste anonime.

   Efficacia: Riduce notevolmente la superficie di attacco, impedendo agli attaccanti di sfruttare connessioni senza credenziali valide.

   Effort: Medio. Configurare correttamente le impostazioni di sicurezza può richiedere una certa competenza e attenzione ai dettagli, ma è un'operazione che, una volta eseguita, richiede poca manutenzione.

3. **Utilizzare firewall e IDS/IPS:** Questi possono essere configurati per rilevare e bloccare tentativi di stabilire Null Sessions.

   Efficacia: Molto alta. Questi strumenti non solo proteggono dalle Null Sessions, ma anche da una vasta gamma di altre minacce.

   Effort: Alto. La configurazione iniziale, la sintonizzazione e la manutenzione continua dei firewall e dei sistemi IDS/IPS possono richiedere una notevole quantità di risorse e competenza.

4. **Monitorare regolarmente:** Monitorare la rete e i sistemi per rilevare tentativi non autorizzati di accesso o attività sospette.

   Efficacia: Alta. Conoscere e rispondere rapidamente alle attività sospette può prevenire danni significativi.

   Effort: Alto. Implementare una solida soluzione di monitoraggio e assicurarsi che venga controllata regolarmente richiede sia risorse tecnologiche che umane.

5. **Aggiornare a versioni più recenti di Windows:** Le versioni più recenti di Windows hanno ridotto o eliminato la vulnerabilità delle Null Sessions.

   Efficacia: Alta. Le versioni più recenti hanno correzioni di sicurezza e caratteristiche che riducono le vulnerabilità.

   Effort: Medio-alto. Aggiornare i sistemi operativi può richiedere test, formazione e potenzialmente l'aggiornamento di altre applicazioni o hardware, ma è un investimento che paga nel lungo termine in termini di sicurezza e funzionalità