Cosa è una Null Session:

Una Null Session è una vulnerabilità che sfrutta un bug nel protocollo di autenticazione NetBIOS di Windows. Permette ad un utente malintenzionato di accedere a risorse di rete senza fornire credenziali di autenticazione. In pratica, l'attaccante si "impersona" come una sessione di autenticazione vuota, sfruttando un'anomalia nel modo in cui Windows gestisce le richieste di accesso.

Sistemi vulnerabili:

Windows NT 4.0

Windows 2000

Windows XP

Windows Server 2003

Esistono ancora?

Windows NT 4.0 è stato rilasciato nel 1996 ed è obsoleto da anni.

Windows 2000 è stato rilasciato nel 2000 ed è obsoleto dal 2010.

Windows XP è stato rilasciato nel 2001 ed è obsoleto dal 2014.

Windows Server 2003 è stato rilasciato nel 2003 ed è obsoleto dal 2015.

Mitigazione e risoluzione:

Disattivare NetBIOS su sistemi non necessari: Se non si utilizza NetBIOS, disattivarlo riduce il rischio di attacco.

Applicare patch di sicurezza: Microsoft ha rilasciato patch per correggere la vulnerabilità Null Session. Assicurarsi che i sistemi siano aggiornati.

Utilizzare autenticazione forte: Implementare l'autenticazione Kerberos o NTLM anziché la semplice autenticazione basata su password.

Limitare l'accesso alle risorse di rete: Limitare l'accesso alle risorse di rete solo agli utenti che ne hanno bisogno.

Commento sulle azioni di mitigazione:

Disattivare NetBIOS:

Efficacia: Alta. Elimina completamente il rischio di attacco Null Session.

Applicare patch di sicurezza:

Efficacia: Alta. Corregge la vulnerabilità alla base dell'attacco.

Utilizzare autenticazione forte:

Efficacia: Molto alta. Rende l'attacco Null Session molto più difficile da realizzare.

Limitare l'accesso alle risorse di rete:

Efficacia: Alta. Riduce l'impatto di un attacco Null Session.

Inoltre si può anche

1. **Aggiornare il sistema operativo:** Se possibile, aggiornare il sistema operativo a una versione più recente e supportata. Versioni più recenti di Windows spesso includono miglioramenti alla sicurezza che riducono il rischio di Null Session.
2. **Configurare correttamente le autorizzazioni:** Limitare rigorosamente le autorizzazioni sui file e sulle directory per evitare l'accesso non autorizzato.
3. **Monitoraggio e rilevamento delle attività sospette:** Implementare strumenti di monitoraggio per individuare e rispondere prontamente a attività anomale, inclusa l'attività Null Session.

L'efficacia di queste azioni di mitigazione dipende dalla situazione specifica e dal contesto aziendale. Disabilitare completamente Null Session può essere efficace, ma potrebbe richiedere un certo sforzo per assicurarsi che le applicazioni e i servizi esistenti funzionino correttamente senza di essa.