Report sulla Vulnerabilità Null Session in Sistemi Windows

Introduzione

La vulnerabilità **Null Session** su Windows è una vulnerabilità di sicurezza che consente a un attaccante di accedere a informazioni sensibili sui sistemi Windows, come nomi di account utente, password e informazioni di condivisione delle risorse. Questa vulnerabilità si verifica quando un client Windows si connette a un server Windows utilizzando un'identità vuota, ovvero senza specificare alcuna credenziale di accesso.

Sistemi Operativi Vulnerabili

La vulnerabilità Null Session colpisce i seguenti sistemi operativi:

- Windows NT
- Windows 2000
- Windows XP
- Windows Server 2003

Tuttavia, è importante notare che è stata risolta in versioni successive dei sistemi operativi Windows e che molti amministratori di sistema di Windows hanno adottato misure di sicurezza per mitigare questa vulnerabilità.

Metodi di Mitigazione

Per mitigare questa vulnerabilità, è possibile adottare i seguenti metodi:

1. **Disabilitare la condivisione file e stampanti su Windows**: eliminare completamente la condivisione su tutti i computer e server della rete. *(Estirpo il problema alla radice, ma le aziende usano la condivisione dei file e non è un'ottima risoluzione)*
2. **Disabilitare il supporto per NetBIOS su TCP/IP**: questo riduce il numero di porte aperte sul sistema e rimuove il supporto per il protocollo NetBIOS che è vulnerabile alla null session.
3. **Utilizzare il filtro del traffico di rete**: firewall bloccano i tentativi di connessione remota non autorizzati e filtrano le connessioni in ingresso sulla base delle porte che tentano di utilizzare. *(Il monitoraggio di rete è una delle pratiche di sicurezza sempre raccomandate)*
4. **Disattivare l'account Guest**: l'account guest consente l'accesso alle risorse della rete senza richiedere alcuna credenziale. Disabilitare l'account Guest può limitare l'accesso di utenti non autorizzati. *(Certamente un'ottima soluzione, da applicare in ogni caso)*
5. **Aggiornare il sistema operativo**: Microsoft rilascia regolarmente gli aggiornamenti di sicurezza per il sistema operativo Windows. Assicurarsi di aver installato l'ultimo aggiornamento di sicurezza per mitigare i rischi di vulnerabilità. *(Con una patch l'effort per l'azienda è basso. Passare ad un sistema operativo più moderno è oneroso a livello di configurazione e richieste hardware)*
6. **Configurare le autorizzazioni di condivisione file**: limita l'accesso alle risorse ai soli utenti specifici che ne hanno bisogno, utilizzando i permessi appropriati. Questo evita il potenziale accesso non autorizzato. *(Certamente un ottimo sistema e una best practice in ogni caso, non sempre applicato nelle aziende medio/piccole)*

7. **Utilizzare un software di sicurezza**: implementare un software di sicurezza per i sistemi Windows che possa monitorare e prevenire l'accesso non autorizzato. *(Fa parte delle soluzioni base da applicare sempre)*

Efficacia ed Effort delle Misure di Mitigazione

Efficacia delle Misure di Mitigazione

Misura di Mitigazione	**Efficacia (0-10)**
Aggiornamento del Sistema Operativo	9
Configurazione delle Politiche di Sicurezza	8
Utilizzo di Firewall e Filtraggio IP	8
Monitoraggio e Auditing	7
Disabilitazione Account Guest	8
Configurazione delle Autorizzazioni	8
Utilizzo di Software di Sicurezza	7

Effort delle Misure di Mitigazione

Misura di Mitigazione	**Effort (0-10)**
Aggiornamento del Sistema Operativo	8
Configurazione delle Politiche di Sicurezza	6
Utilizzo di Firewall e Filtraggio IP	5
Monitoraggio e Auditing	5
Disabilitazione Account Guest	3
Configurazione delle Autorizzazioni	4
Utilizzo di Software di Sicurezza	5

Conclusioni

La vulnerabilità della Null Session è stata una significativa minaccia di sicurezza per i vecchi sistemi Windows. Sebbene molti di questi sistemi non siano più supportati, la presenza di ambienti legacy rappresenta ancora un rischio. L'adozione di misure di mitigazione come l'aggiornamento dei sistemi, la configurazione delle politiche di sicurezza, l'uso di firewall e il monitoraggio attivo può proteggere efficacemente contro questa vulnerabilità. La scelta della misura da adottare dipenderà dall'ambiente specifico e dalle risorse disponibili dell'organizzazione.