Esercitazione 7 Modulo 4 – Alessio Russo

Nella lezione teorica abbiamo visto la Null Session, vulnerabilità che colpisce Windows
Traccia
• Spiegare brevemente cosa vuol dire Null Session
• Elencare i sistemi che sono vulnerabili a Null Session
• Questi sistemi operativi esistono ancora oppure sono estinti da anni e anni?
• Elencare le modalità per mitigare o risolvere questa vulnerabilità
• Commentare queste azioni di mitigazione, spiegando l'efficacia e l'effort per l'utente/azienda.

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. La vulnerabilità Null Session colpisce i sistemi operativi Windows NT, Windows 2000, Windows XP e 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.

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

- 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
- 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.
- Utilizzare i firewall bloccano i tentativi di connessione remota non autorizzati e filtrano le connessioni in ingresso sulla base delle porta che tentano di utilizzare. Il monitoraggio di rete è una delle pratiche di sicurezza sempre raccomandate
- 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

- 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 pach l'effort per l'azienda è basso. Passare ad un sistema operativo più moderno è oneroso a livello di configurazione e richieste hardware

- 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

- 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.