Null Session, Vulnerabilità nei Sistemi Operativi

W15-D2

1. **Cosa vuol dire Null Session?**

- Definizione: Una Null Session è una connessione a un sistema remoto utilizzando una sessione di rete senza autenticazione, consentendo l'accesso anonimo
- Le NetBIOS null sessions sono vulnerabilità trovate nel SMB (Server Message Block) dei sistemi operativi Windows (spesso versioni «legacy» o obsolete e non più supportate), che lavora nella porta TCP 139 SMB NetBIOS, e possiamo trovarle anche nel Common Internet File System (CIFS). Questi due protocolli permettono infatti di operare su file remoti come se risiedessero in locale.

2. **Sistemi vulnerabili alle Null Sessions**

Tra i sistemi operativi vulnerabili a questa problematica abbiamo:

1. ***Windows 95***, uno dei primi sistemi operativi con una GUI avanzata che supportava la rete, incluse le Null Sessions per la condivisione semplice delle risorse.
2. ***Windows 98,*** Sistema operativo destinato agli utenti domestici e alle piccole imprese, vulnerabile alle Null Sessions per le sue impostazioni di rete.
3. ***Windows NT***, uno dei primi sistemi operativi Windows a supportare la rete e la condivisione di risorse.
4. ***Windows ME (Millennium Edition),*** anche se meno utilizzato, questo sistema operativo era vulnerabile alle Null Sessions simili ai suoi predecessori.
5. ***Windows 2000,*** successore di Windows NT, mantiene molte delle stesse configurazioni di rete, inclusa la vulnerabilità alle Null Sessions.
6. ***Windows XP,*** popolare sistema operativo per desktop, vulnerabile nelle configurazioni predefinite che permettono l'accesso anonimo per semplificare la condivisione di risorse.

3. **Modalità di mitigazione e risoluzione**

Purtroppo molti di questi sistemi operativi sono diventati obsoleti e non più supportati ufficialmente da Microsoft, ma spesso e volentieri vengono usati in ambienti «legacy» da chi non vuole o non può fare upgrade di sistema operativo. Le implementazioni da fare nel nostro ambiente lavorativo sono:

1. ***Aggiornamenti del Sistema***: Passare a versioni più recenti e supportate dei sistemi operativi come Windows 10 o 11.
2. ***Configurazioni di Sicurezza***: Disabilitare le Null Session tramite le impostazioni di registro e policy di gruppo ed implementare e configurare firewall per bloccare accessi non autorizzati alle porte 137 a 139 TCP, da 137 a 139 UDP, 445 TCP e 445 UDP.
3. ***Monitoraggio e Controllo***: Implementare un Intrusion Detection System(IDS) per monitorare tentativi di accesso anonimi. Verificare regolarmente i log di sistema per attività sospette ed in caso prendere provvedimenti per bloccare i tentativi.

4. **Efficacia delle azioni di mitigazione**

1. *Aggiornamenti del Sistema:*

- **Efficacia**: Alta, risolve alla radice la vulnerabilità.
- **Effort**: Alto, richiede tempo e molte risorse per la migrazione soprattutto se si passa da sistemi obsoleti e retrodatati.

2. *Configurazioni di Sicurezza:*

- **Efficacia**: Media, riduce significativamente il rischio ma non lo elimina del tutto.
- **Effort**: Medio, richiede conoscenze tecniche per configurazioni corrette senza commettere errori.

3. *Monitoraggio e Controllo:*

- **Efficacia**: Alta, permette di individuare e rispondere rapidamente alle minacce.
- **Effort**: Variabile, dipende sempre dalla complessità del sistema di monitoraggio implementato.

5. **Conclusioni**

- ***Riepilogo***: Le null sessions presentano un grandissimo problema e vulnerabilità ma solo nei sistemi operativi obsoleti e non più usati, portando all'esposizione di dati sensibili presenti nella macchina sfruttando una falla nel sistema.
- ***Raccomandazioni***: Si consiglia quindi la migrazione a sistemi più recenti, l'utilizzo di configurazioni di sicurezza adeguate e un monitoraggio costante, al fine di proteggere efficentemente le reti aziendali.